



FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS

DISEÑO E IMPLEMENTACIÓN DE UN AGENTE DE ADMINISTRACIÓN,  
CONFIGURACIÓN Y MONITOREO PARA DISPOSITIVOS DE RED  
CISCO

AUTOR

CARLOS ANDRÉS VACAS ANDRADE

AÑO

2019



FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

DISEÑO E IMPLEMENTACIÓN DE UN AGENTE DE ADMINISTRACIÓN,  
CONFIGURACIÓN Y MONITOREO PARA DISPOSITIVOS DE RED CISCO

Trabajo de Titulación presentado en conformidad con los requisitos establecidos  
para optar por el título de Ingeniero Electrónico y Redes de Información

Profesor Guía

Mg. Iván Patricio Ortiz Garcés

Autor

Carlos Andrés Vacas Andrade

Año

2019

## **DECLARACIÓN DEL PROFESOR GUÍA**

“Declaro haber dirigido el trabajo, Diseño e implementación de un agente de administración, configuración y monitoreo para dispositivos de red Cisco, a través de reuniones periódicas con el estudiante Carlos Andres Vacas Andrade, en el Semestre 201920, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

---

Iván Patricio Ortiz Garcés  
Magister en Redes de Comunicaciones  
CC: 0602356776

## **DECLARACIÓN DEL PROFESOR CORRECTOR**

“Declaro haber revisado este trabajo, Diseño e implementación de un agente de Administración, Configuración y Monitoreo para dispositivos de red Cisco, del estudiante Carlos Andres Vacas Andrade, en el semestre 201920, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

---

William Eduardo Villegas Chilibuina  
Magister en Redes de Comunicaciones  
CC: 1715338263

## **DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE**

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

---

Carlos Andrés Vacas Andrade

CC: 1723522171

## **AGRADECIMIENTOS**

Agradezco el apoyo incondicional de mi madre, quien ha permitido que pueda efectuar mis estudios de educación superior y quien me ha formado como una persona de bien.

## RESUMEN

La elaboración del presente trabajo tiene como propósito el diseño, desarrollo e implementación de un agente de gestión y monitoreo, para dispositivos de red tradicionales (modelo de red jerárquico). El sistema propuesto pretende aumentar el grado de simplicidad de administración de dispositivos Cisco, al centralizar los nodos de una red, mediante una interfaz gráfica amigable con el usuario final. De esa manera, aumenta el grado de eficiencia y a su vez, reduce los costos operativos.

Se realiza un análisis basado en las configuraciones básicas de los dispositivos Cisco, con el objeto de establecer los parámetros necesarios para llevar a cabo el diseño de interfaces gráficas. Las interfaces que se diseñan le permiten al usuario final configurar de manera fácil y sin necesidad de conocimiento profundo del sistema operativo de Cisco IOS.

Se agrega funcionalidad a las formas de Windows, a partir de la utilización de programación orientada a objetos. Se establecen atributos a las clases, las cuales describen lógicamente a los dispositivos e interactúan con las funciones y las formas. Además, se utilizan protocolos nativos de los dispositivos Cisco, mediante los cuales se establecen las comunicaciones necesarias entre las interfaces del dispositivo de red y el ordenador donde se aloja el sistema de gestión. Se agrega también, un módulo para la verificación del estado de los equipos.

La implementación inicial de la solución se realiza en un medio virtual, el cual es necesario para el desarrollo de la solución. Así también se implementa un medio físico, una sencilla infraestructura de red, que posibilita las pruebas in situ de las funciones del sistema.

## **ABSTRACT**

The purpose of the following is the design, development and implementation, of a management and monitoring agent designed for traditional networks (hierarchical network model). The proposed system is intended to augment the management simplicity degree for Cisco networking devices, by centralizing network nodes through the usage of a friendly GUI (Graphical User Interface). Allowing to achieve an improved degree of efficiency and reduction of operative expenses.

A basic analysis based on Cisco devices configuration is created, in order to establish necessary parameters to accomplish the design of graphic user interfaces. These graphical interfaces to be designed, allow the final user to easily configure Cisco IOS without the necessity of deep knowledge about this operative system.

Functionality is added to the windows forms through object-oriented programming. Attributes are established in relation to classes, which logically describe the devices and interact with the functions and graphical forms. Moreover, Cisco devices native protocols are used in furtherance of establish the necessary communications between the network devices and the server that withholds the managing system. A module to check the equipment status, is also added.

The solution's implementation is made through a virtual environment, which is necessary for the development of the solution. Also, a physical setting is implemented, a simple network infrastructure, which allows in site testing of system functionalities.



# ÍNDICE

1.	CAPITULO I: INTRODUCCIÓN .....	1
1.1.	ALCANCE .....	2
1.2.	JUSTIFICACIÓN .....	2
1.3.	OBJETIVOS .....	3
1.3.1.	OBJETIVO GENERAL.....	3
1.3.2.	OBJETIVOS ESPECIFICOS .....	3
2.	CAPITULO II: MARCO TEÓRICO .....	4
2.1.	Protocolo de red .....	4
2.1.1.	SSH .....	4
2.1.2.	SNMP .....	4
2.1.2.1.	Agente SNMP .....	5
2.1.2.2.	Administrador SNMP.....	5
2.2.	Red de computación.....	6
2.2.1.	Interfaz de red.....	6
2.2.2.	Ethernet.....	7
2.2.3.	Comunicación serial .....	7
2.2.4.	Direccionamiento IP.....	8
2.3.	Conmutador .....	8
2.3.1.	VLAN .....	9
2.3.2.	VLAN troncales.....	9
2.4.	Enrutador.....	9
2.5.	Sistema operativo .....	10
2.6.	Cisco IOS .....	11
2.7.	Infraestructura de tecnologías de la información.....	11
2.7.1.	Servidor .....	11
2.7.2.	Modelo de infraestructura .....	12

2.7.3.	Seguridad .....	12
2.7.4.	Disponibilidad .....	12
2.7.5.	Escalabilidad.....	13
2.8.	Virtualización .....	13
2.8.1.	Hipervisor .....	13
2.8.1.1.	Hipervisor tipo 1 .....	14
2.8.1.2.	Hipervisor tipo 2 .....	15
2.9.	Interfaz de línea de comandos.....	16
2.10.	Interfaz gráfica de usuario.....	16
2.11.	Microsoft Visual Studio .....	17
2.11.1.	Formas de Windows.....	17
2.12.	Programación orientada a objetos .....	18
2.12.1.	Clase .....	19
<b>3.</b>	<b>CAPITULO III: ANÁLISIS CONDICIONES INICIALES .....</b>	<b>19</b>
3.1.	Modos de operación Cisco IOS .....	20
3.2.	Estructura de comandos IOS .....	21
3.3.	Análisis enrutador .....	22
3.3.1.	Configuraciones iniciales .....	22
3.3.2.	Configuraciones de interfaces LAN .....	23
3.3.3.	Configuraciones de seguridad .....	23
3.3.3.1.	Configuraciones de acceso EXEC privilegiado .....	24
3.3.3.2.	Configuraciones de líneas VTY .....	24
3.3.4.	Configuraciones SSH .....	25
3.3.5.	Configuraciones de enrutamiento RIP .....	26
3.3.6.	Configuraciones de servidor DHCP .....	27
3.3.7.	Configuraciones de subinterfaces.....	27
3.4.	Análisis conmutador .....	28
3.4.1.	Configuraciones iniciales .....	28

3.4.2.	Configuraciones de interfaz de manejo .....	29
3.4.3.	Configuraciones SSH .....	30
3.4.4.	Configuraciones VLAN .....	31
3.4.5.	Configuraciones puerto troncal y acceso.....	32
3.4.6.	Seguridad de Puertos .....	33
4.	<b>CAPITULO IV: DISEÑO DE INTERFACES</b> .....	34
4.1.	Terminal serial.....	35
4.2.	Terminal SSH.....	36
4.3.	Diseño de interfaces de enrutador .....	37
4.3.1.	Agente de agregación.....	37
4.3.2.	Agente de configuración .....	40
4.3.2.1.	Inicio de sesión .....	40
4.3.2.2.	Pantalla de configuración.....	41
4.4.	Diseño de interfaces de conmutador .....	44
4.4.1.	Agente de agregación.....	45
4.4.2.	Agente de configuración .....	48
4.4.2.1.	Inicio de sesión .....	48
4.4.2.2.	Pantalla de configuración .....	49
4.5.	Agente de monitoreo .....	52
4.6.	Infraestructura .....	53
5.	<b>CAPITULO V: IMPLEMENTACIÓN Y PRUEBAS</b> .....	58
5.1.	Incorporación de dispositivos .....	60
5.2.	Configuración de dispositivos.....	67
5.2.1.	Router de borde.....	67
5.2.2.	Switch de acceso 1 .....	70
6.	<b>CONCLUSIONES Y RECOMENDACIONES</b> .....	72
6.1.	CONCLUSIONES .....	72
6.2.	RECOMENDACIONES.....	74

REFERENCIAS .....	75
ANEXOS .....	80

## ÍNDICE DE FIGURAS

Figura 1. Diagrama Funcional SNMP.....	5
Figura 2. Modelo Primitivo de Red de Computación.....	6
Figura 3. Interfaces de Dispositivo de Red Cisco.....	6
Figura 4. Interfaz Ethernet.....	7
Figura 5. Interfaz Serial RS-232/USB.....	8
Figura 6. Switch Cisco 2960.....	9
Figura 7. Enrutador Cisco 2900.....	10
Figura 8. Definición Gráfica de Sistema Operativo.....	11
Figura 9. Diagrama de Bloques de Hipervisor.....	14
Figura 10. Diagrama de Bloques de Hipervisor Tipo 1.....	15
Figura 11. Diagrama de Bloques Hipervisor Tipo 2.....	16
Figura 12. Captura CLI.....	16
Figura 13. Interfaz Gráfica de Usuario Windows 8.....	17
Figura 14. Ventana de Visual Studio.....	18
Figura 15. Diagrama de Clase y Objetos.....	19
Figura 16. Modelo Cascada, Fase Análisis de Condiciones Iniciales.....	20
Figura 17. Modelo de Estructura Jerárquica de Modos de IOS.....	21
Figura 18. Diagrama de Sintaxis de Comandos IOS.....	22
Figura 19. Modelo Cascada.....	35
Figura 20. Ventana Terminal Serial.....	36
Figura 21. Ventana Terminal SSH.....	36
Figura 22. Dialogo de Permiso Denegado.....	37
Figura 23. Pantalla de Bienvenida.....	37
Figura 24. Pantalla de Conexión.....	38
Figura 25. Pantalla de Parámetros de Red.....	39
Figura 26. Pantalla de Parámetros de Seguridad.....	39
Figura 27. Ventana de Inicio de Sesión.....	40
Figura 28. Ventana de Acceso Verificado.....	40
Figura 29. Ventana de Acceso Denegado.....	41
Figura 30. Ventana de Configuración General.....	41
Figura 31. Ventana de Configuración Inicial.....	42
Figura 32. Ventana de Configuración de Interfaz.....	42
Figura 33. Ventana de Configuración de RIP.....	43
Figura 34. Ventana de Configuración de DHCP.....	44
Figura 35. Ventana de Configuración de Subinterfaces.....	44
Figura 36. Pantalla de Bienvenida.....	45

Figura 37. Pantalla de Conexión Serial .....	46
Figura 38. Dialogo de Verificación.....	46
Figura 39. Ventana Configuración de Interfaz SVI. ....	47
Figura 40. Ventana de Configuración de Seguridad.....	47
Figura 41. Pantalla de Inicio de Sesión .....	48
Figura 42. Pantalla de Acceso Permitido .....	48
Figura 43. Pantalla de Acceso Denegado. ....	49
Figura 44. Pantalla de Configuración General.....	49
Figura 45. Pantalla de Configuración Inicial. ....	50
Figura 46. Pantalla de Configuración VLAN.....	51
Figura 47. Pantalla de Configuración de Puertos Troncales. ....	52
Figura 48. Pantalla de Monitoreo .....	52
Figura 49. Extracción de Máquina Virtual.....	53
Figura 50. Importe de Máquina Virtual. ....	54
Figura 51. Inicio de Sesión en Máquina Virtual. ....	54
Figura 52. Ejecución de Comando Terminal. ....	55
Figura 53. Acceso Desde WinSCP.....	55
Figura 54. Panel de Administración de Máquinas Virtuales. ....	56
Figura 55. Creación de Puerto Serial. ....	56
Figura 56. CLI Putty. ....	57
Figura 57. Diagrama de Implementación. ....	57
Figura 58. Modelo Cascada .....	58
Figura 59. Diagrama Topológico Red Simulada.....	59
Figura 60. Topología Física.....	60
Figura 61. Ejecución de Comandos. ....	60
Figura 62. Configuración de Red PC.....	61
Figura 63. Pantalla de Bienvenida.....	62
Figura 64. Configuración de SVI. ....	62
Figura 65. Verificación de la Ejecución. ....	63
Figura 66. Configuración de Parámetros de Seguridad y Validación. ....	64
Figura 67. Ventana de Bienvenida .....	65
Figura 68. Ventana de Comunicación Serial. ....	65
Figura 69. Configuraciones de Interfaz de Red y Validación.....	66
Figura 70. Configuraciones de Parámetros de Seguridad y Validación. ....	66
Figura 71. Conectividad LAN.....	67
Figura 72. Inicio de Sesión.....	68
Figura 73. Configuración de Interfaces. ....	68
Figura 74. Configuración de Subinterfaces. ....	69
Figura 75. Configuración DHCP.....	69

Figura 76. Configuración de Router RIP. ....	70
Figura 77. Inicio de Sesión.....	70
Figura 78. Configuración de VLAN.....	71
Figura 79. Configuración de Enlace Troncal. ....	71

## ÍNDICE DE TABLAS

Tabla 1. Configuraciones Iniciales de Enrutador .....	22
Tabla 2. Configuración de Interfaz de Red de Enrutador .....	23
Tabla 3 Configuraciones de Acceso EXEC Privilegiado de Enrutador .....	24
Tabla 4. Configuraciones de Líneas VTY de Enrutador .....	25
Tabla 5. Configuraciones SSH de Enrutador.....	25
Tabla 6. Configuraciones de Enrutamiento RIP .....	26
Tabla 7. Configuraciones de Servidor DHCP .....	27
Tabla 8. Configuraciones de Subinterfaces de Enrutador .....	28
Tabla 9. Configuraciones Iniciales de Conmutador .....	28
Tabla 10. Configuraciones de Interfaz de Manejo de Conmutador .....	29
Tabla 11. Configuraciones SHH de Conmutador .....	30
Tabla 12. Configuraciones de VLAN .....	31
Tabla 13. Configuraciones de Puerto de Acceso .....	32
Tabla 14. Configuraciones de Puerto Troncal .....	33
Tabla 15. Configuraciones de Seguridad de Puertos .....	34



## 1. CAPITULO I: INTRODUCCIÓN

“El mercado de las redes definidas por software (SDN) espera llegar a los 61 Bn. de dólares norteamericanos para el 2023”, como lo menciona un artículo de Market Watch (Market Watch, 2019, Recuperado de: [www.marketwatch.com](http://www.marketwatch.com)). Uno de los factores que aporta a tal extensión en el mercado, es su precisión y consistencia en las operaciones de configuración. Por el contrario de las redes tradicionales, las cuales no sólo son complicadas de configurar, sino que también dan cabida al cometimiento de errores. Es claro que el aumento de seguridad también es significativo en redes “SDN”, respecto de las redes jerárquicas. Esto se debe a la gran cantidad de configuraciones individuales, requeridas para evitar vulnerabilidades de seguridad de la información.

Así como se menciona (Tanburn y Didar, 2001, pp. 9-12), la instalación de infraestructura está estrechamente relacionada con los costos de acceso a las Tecnologías de la Información y Comunicación, lo cual, es un problema mayor en los países en vías de desarrollo, dado que las nuevas tecnologías de red definidas por software son significativamente más costosas que las infraestructuras de red tradicionales; es poco probable que las empresas en los países en vías de desarrollo decidan implementar estas nuevas tecnologías, a pesar de las ventajas que “SDN” provee.

Teniendo en cuenta las condiciones anteriormente mencionadas, se encuentra un nicho de mercado, para aquellas empresas que no están dispuestas a adquirir infraestructuras de red del tipo “software defined”, pero si están interesadas en mejorar sus procesos de administración de red, en sus ya existentes infraestructuras jerárquicas Cisco. Lo cual se logra, mediante la implementación del agente de administración, configuración y monitoreo para dispositivos de red Cisco.

## **1.1. ALCANCE**

Diseñar un programa con interfaz de usuario en Microsoft Visual Studio, en el lenguaje de programación C#, con la posibilidad de ejecutar comandos a nivel de consola, mediante SSH, para comunicarse de manera automática con los dispositivos de red Cisco que se encuentren conectados y monitorearlos a través SNMP. A continuación, se explican las especificaciones en detalle:

El programa contiene varios módulos necesarios para su operación. Primero, dispone de un “wizard” de configuración, es decir un agente, el cual especifica los parámetros iniciales necesarios para comunicarse con el programa, dentro del equipo Cisco. Adicionalmente, habilita un menú donde se encuentran los parámetros requeridos de configuración y permite a través del protocolo SSH, establecer esos parámetros en los dispositivos correspondientes.

Además, tiene un módulo capaz de generar archivos de respaldo de la configuración de los dispositivos agregados al programa. Dichos archivos se almacenan con el propósito de reestablecer las configuraciones del dispositivo, de ser necesario. Por último, cuenta con un monitor de los dispositivos de red activos, mediante el uso de protocolo SNMP, este envía una alerta al administrador en el caso de haber pérdidas de conectividad.

## **1.2. JUSTIFICACIÓN**

La falta de una herramienta que permita a los administradores de TI configurar de manera sencilla los dispositivos activos de la red y permita la centralización de las tareas necesarias de configuración, agilizando, optimizando y aumentando la seguridad de la red. Adicionalmente, se incrementa la integridad de la red al brindar la posibilidad de almacenar archivos de respaldo de la configuración en caso de

fallo de equipos o mantenimiento. El monitoreo centralizado otorgado por la herramienta en cuestión permite también la gestión proactiva oportuna.

### **1.3. OBJETIVOS**

#### 1.3.1. OBJETIVO GENERAL

Desarrollar un programa en Microsoft Visual Studio en lenguaje C# que sirva como agente de configuración y monitoreo para dispositivos de red Cisco.

#### 1.3.2. OBJETIVOS ESPECIFICOS

- Analizar las variables en función de los parámetros de configuración de los equipos, con el propósito de generar un reporte inicial.
- Diseñar las interfaces gráficas que componen la solución, teniendo presentes las variables recopiladas en el análisis preliminar, y sus respectivas funcionalidades.
- Probar sobre equipos físicos, para examinar las distintas funcionalidades de la solución.

## 2. CAPITULO II: MARCO TEÓRICO

### 2.1. Protocolo de red

Se puede definir como un conjunto de reglas por las cuales se comunican los componentes de un sistema. Debido a que en una red de comunicaciones existe cierta complejidad en la coordinación de las operaciones, es necesario establecer protocolos para mitigar los posibles errores. Cada protocolo define su manera de interpretar la información y la transaccionalidad que utiliza. Existen diversos protocolos dependiendo del nivel de comunicación. (Silverschatz, 2006, pp. 572-573)

#### 2.1.1. SSH

El "Secure Shell" (SSH) es un protocolo que provee un manejo de conexión cifrado hacia un dispositivo remoto. Permite la administración de un componente de red a través de la línea de comandos. Posee cifrado fuerte y autenticación (Usuario y Contraseña), aumentando el grado de seguridad de la transferencia. Utiliza el puerto 22 para establecer la comunicación. (Cisco Netacad, 2019).

#### 2.1.2. SNMP

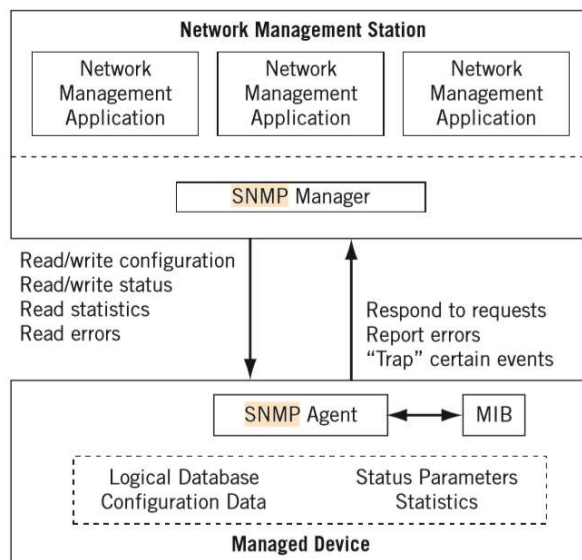
Es un protocolo que permite administrar los componentes de red. Aumenta el grado de seguridad de la red, al permitir el monitoreo constante de los dispositivos de red y las funciones que habilitan. Provee un lenguaje común para elementos de red que les permite remitir información dentro de redes con dispositivos de diversas marcas. Las versiones más recientes de SNMP, incluyen mejoras de seguridad, como autenticación y cifrado de los mensajes SNMP. El protocolo de SNMP está compuesto de diversos componentes:

### 2.1.2.1. Agente SNMP

Es el programa que se ejecuta sobre el sistema que se ha de monitorear, colecciona la información de estado de dicho sistema y se envía hacia el administrador SNMP. Adicionalmente, le puede enviar alertas reactivas o proactivas al SNMP, si encuentra errores. La mayoría de los dispositivos contienen agentes preinstalados, los cuales deben ser activados y configurados.

### 2.1.2.2. Administrador SNMP

Es un software que recoge la información enviada por los agentes y la procesa. Activamente, solicita a los agentes que envíen información en intervalos regulares. Lo que le permite al administrador de la red encontrar defectos y repararlos o prevenirlos. Los administradores de SNMP son de vital importancia en empresas que contienen miles de nodos de red. (Goralski, 2009, pp. 612). A continuación, se observa un diagrama funcional de SNMP.

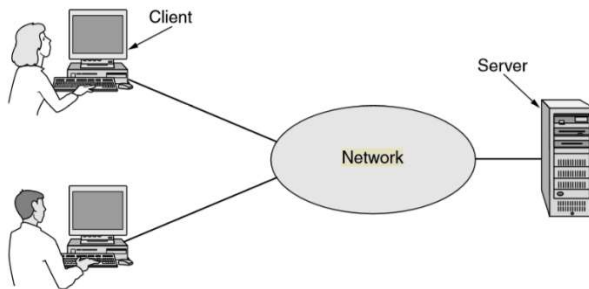


*Figura 1.* Diagrama Funcional SNMP

Tomada de: Goralski, 2009, pp. 612.

## 2.2. Red de computación

Es un gran número de computadores interconectados por una tecnología. Se dice que dos computadores están interconectados si son capaces de intercambiar información. Las tecnologías de comunicación son diversas: fibra óptica, microondas, infrarrojo e incluso tecnologías satelitales. La internet es la red de redes de computadoras más ampliamente conocida. (Tanenbaum, 2009, pp.2-4). En la figura a continuación se observa un diagrama de red simplificado.



*Figura 2. Modelo Primitivo de Red de Computación.*

Tomada de: Goralski, 2009, pp. 3

### 2.2.1. Interfaz de red

Son puertos especializados en un dispositivo de red que conectan a redes individuales (Figura 3). Debido a que los enrutadores interconectan redes, se los conoce como interfaces de red. (Cisco NetAcad, 2019).

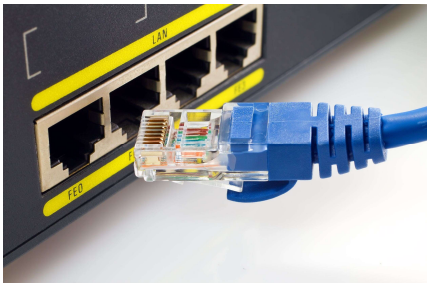


*Figura 3. Interfaces de Dispositivo de Red Cisco*

Tomada de: Cisco s.f.

### 2.2.2. Ethernet

Según se describe en el Estándar IEEE 802.3, es una tecnología que consiste en un cable al cual se conectan varias computadoras. Este cable es reconocido como Ethernet y permite la comunicación entre los nodos de red (Figura 4). Los cables Ethernet tienen una longitud máxima y capacidad de implementación y es debido a que, al exceder cierta longitud y tráfico, existe pérdida de información. Cada equipo de red tiene un puerto Ethernet, el cual es conectado a un "Switch", que a su vez se encarga de conmutar la información hacia su destino. (Goralski, 2009, p.87-89)



*Figura 4. Interfaz Ethernet*

Tomada de: Digitaltrends s.f.

### 2.2.3. Comunicación serial

La comunicación serial puede ocurrir a través de un puerto RS-232 o a través de un Universal Serial Bus (USB). Un puerto serial es una interfaz de computadora que transmite información un bit a la vez. La mayoría de los puertos son bidireccionales, es decir pueden enviar y recibir información. En general la expresión se refiere a la utilización de un protocolo asíncrono. Tiene ciertas desventajas de velocidad y distancia al transmitir un bit a la vez, pero a su vez, es posible implementar cables y conectores de bajo costo. Para programación en Microsoft .NET se puede utilizar la librería de clases "SerialPort" para acceder a los puertos COM. Algunos dispositivos de red pueden funcionar como servidores seriales, permitiendo el acceso de puertos seriales a través de la red. (Axelson, 2007, pp. 1-3)



*Figura 5.* Interfaz Serial RS-232/USB

#### 2.2.4. Direccionamiento IP

Una dirección IP refiere a “Internet Protocol” y es una etiqueta numérica que se le asigna a cada host o nodo en una red. Se encarga de habilitar la comunicación entre los elementos de una red Ethernet. Existen dos versiones de direccionamiento IP, IPv4 que se compone de números binarios de 32 bits, e IPv6 como una versión mejorada de IPv4 de 128 bits. Las direcciones IP les permiten a los elementos de una red identificar una fuente y un destino de la información. La mayoría de los dispositivos puede obtener una IP por interfaz, pero algunos tienen varias interfaces. (Tanenbaum, 2009, pp. 442-445)

### 2.3. Conmutador

Es un nodo de red que reenvía los paquetes hacia un destino dependiendo de la identificación del destino que tenga el paquete. Esta ruta trazada se denomina circuito virtual y se configura por un protocolo de señalización, un circuito virtual conmutado (SVC). Una conexión de este tipo es una asociación lógica entre dos puntos finales. Los paquetes en una red conmutada ofrecen garantía de llegada. Se aprovecha el ancho de banda al implementar procesamiento de paquetes, lo que permite un buen ancho de banda y retraso reducido (Goralski, 2009, p.324-326). Se observa la Figura 6.



### 2.3.1. VLAN

Es una tecnología utilizada para separar el rendimiento de la red, al separar los dominios grandes de “broadcast” en secciones más pequeñas. En su mayoría es una tecnología que se utiliza en redes locales, se incorpora en el diseño de la red y permite soportar los diversos servicios que se transportan en la red. Consiste en agrupar varios dispositivos en una misma red, como si estuviesen conectados al mismo cable, separando las interfaces del “switch” en secciones de red. (Cisco NetAcad, 2019)

### 2.3.2. VLAN troncales

Es un enlace punto a punto entre dos dispositivos de red que manejan mas de una VLAN. Esto les permite a los dispositivos entender las VLANS de los otros conmutadores. El estándar utilizado por Cisco es el IEEE 802.1Q. (Cisco NetAcad, 2019)



*Figura 6.* Switch Cisco 2960

Tomada de: Cisco s.f.

## 2.4. Enrutador

Un enrutador o “router”, es una computadora especializada, que conforma un nodo de red. Este nodo de red remite paquetes hacia un destino, basándose en una dirección única. Esto lo realiza sobre un camino dinámico que puede cambiar

dependiendo del paquete, pero que usualmente es estable en el tiempo. Los paquetes son chequeados solamente si es necesario. Las redes de enrutamiento de paquetes ofrecen solamente entrega de mejor esfuerzo, quiere decir que no garantiza ancho de banda y retardo. Los enrutadores Cisco utilizan IOS como sistema operativo principal. (Cisco Netacad, 2019). En la figura 7 siguiente, se observa un equipo Cisco 2900.

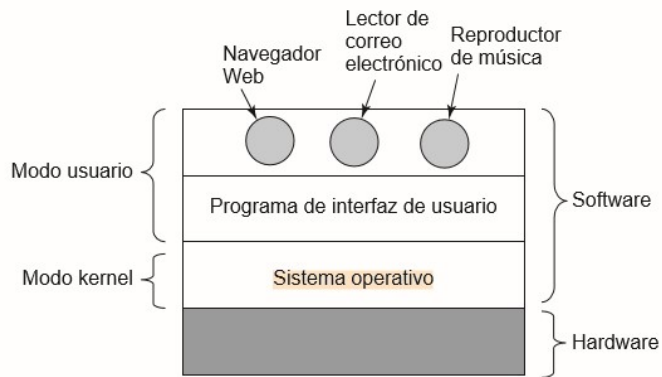


*Figura 7.* Enrutador Cisco 2900

Tomada de: Cisco s.f.

## **2.5. Sistema operativo**

Un sistema operativo es un programa que actúa como intermediario entre el usuario final y el hardware de un ordenador. Su propósito es proporcionar un entorno en el cual el usuario pueda ejecutar programas. El objetivo principal de un sistema operativo es lograr que el sistema de computación se use de manera cómoda; y, el objetivo secundario es que el hardware del computador se emplee de manera eficiente. Tiene dos componentes, el programa con el cual interactúan los usuarios y el núcleo que administra el hardware. El programa que interactúa con el usuario puede ser un GUI, cuando se trata de un ambiente gráfico, o un Shell cuando está basado en texto. (Silverschatz, 2006, pp. 3-5). Se identifica en la figura 8 un diagrama funcional de sistema operativo.



*Figura 8.* Definición Gráfica de Sistema Operativo

Tomada de: Tanenbaum, 2009, pp. 4

## 2.6. Cisco IOS

El "Cisco Internetwork Operating System" es un sistema operativo que se ejecuta en la mayoría de los sistemas Cisco, enrutadores y conmutadores. La función de este sistema operativo es habilitar la comunicación entre los nodos de red. Brinda las herramientas necesarias para interactuar con las interfaces del equipo local y configurarlas. (Cisco Netacad, 2019)

## 2.7. Infraestructura de tecnologías de la información.

Es el conjunto de equipos, sistemas, software y servicios que se utilizan en una organización, independiente de la misión, programa o proyecto. Sirve como la fundación sobre la cual se construyen los sistemas y sus componentes. Está escondido de los usuarios de aplicación, pero es parte importante para el funcionamiento de las utilidades de una compañía. (Laan, 2017, pp.22-23).

### 2.7.1. Servidor

Es un equipo computacional que comparte recursos con los clientes, a través de un protocolo de comunicaciones. En un modelo cliente-servidor, el servidor es quien

entrega la información o los servicios y el cliente es quien solicita y recibe. Los servidores físicos son distintos de los computadores tradicionales, de la manera que tienen hardware preparado para estar operativo de manera continua. Si existe algún fallo en algún componente, este está respaldado por otros componentes similares y es posible reemplazarlo sin mayor complicación. Existen diferentes tipos de servidores. Por ejemplo: un servidor de almacenamiento permite guardar información de manera segura. Un servidor web responde a peticiones de los clientes que solicitan paginas desde un explorador web. Un servidor de base de datos almacena la información de manera estructurada. En concreto las tareas de un servidor son específicas y se dedica solamente a cumplir dichas tareas. (Goralski, 2009, p.55-57)

#### 2.7.2. Modelo de infraestructura

Es un modelo que permite tener un panorama ideal de cómo se organizan los componentes de un sistema óptimo. Ajustarse a este modelo, a su vez, posibilita diseñar un sistema de la mejor manera posible. (Laan, 2017, pp.26-28)

#### 2.7.3. Seguridad

Tiene que ver con el manejo de riesgos, básicamente si no hay riesgos, no hay necesidad de implementar seguridad. El manejo de riesgos consiste en determinar niveles de riesgo aceptables, mitigar los riesgos hasta ese nivel y mantenerlos de esa manera. Los riesgos pueden presentarse en todos los niveles del modelo, por lo cual es necesario tomar las precauciones pertinentes.

#### 2.7.4. Disponibilidad

Refiere al tiempo que un sistema se encuentra disponible. En contraste, el tiempo que el sistema no se encuentra disponible, se denomina “downtime” o tiempo de inactividad. Existen diversos mecanismos para reducir tiempos de baja, utilizar

varios dispositivos en un mismo nodo, implementar tecnología que balancee la carga de trabajo y sistemas de detección de fallos. A pesar de estos mecanismos, eliminar en un 100% los tiempos de baja, es imposible.

#### 2.7.5. Escalabilidad

Indica el nivel de complejidad para modificar un sistema, agregar un nuevo componente o manejar incremento de carga. Un sistema que mejora su capacidad al agregar nuevo hardware, proporcional a la capacidad agregada, se considera escalable. Existen dos maneras de agregar escalabilidad a un sistema: escalabilidad vertical y horizontal. La escalabilidad vertical refiere a agregar más componentes en un mismo equipo, aumentando de esa manera su capacidad. Por otro lado, el escalamiento horizontal tiene que ver con agregar más equipos en un mismo nodo.

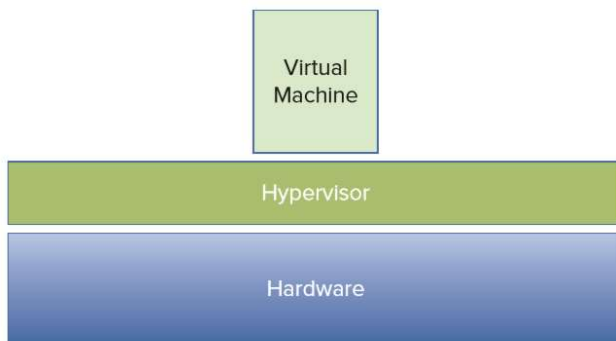
### 2.8. Virtualización

En tecnologías de la información virtualización refiere a la abstracción de algún componente físico, en un objeto lógico. Al virtualizar un objeto, se puede obtener mayor utilidad del recurso que ese objeto provee. Por ejemplo, una red local provee mejor rendimiento y manejo mejorado, cuando se separa del hardware físico. Asimismo, redes de almacenamiento (SAN) proveen gran flexibilidad, disponibilidad mejorada, y uso más efectivo de recursos de almacenamiento, al abstraer los dispositivos físicos en objetos lógicos. La virtualización puede realizarse sobre computadores completos y se puede disponer de varios equipos virtuales sobre un servidor físico. Las instalaciones se realizan en un espacio reservado del servidor físico y son gestionados a través de un hipervisor. (Portnoy, 2017, pp. 2-4)

#### 2.8.1. Hipervisor

Tradicionalmente conocido como Monitor de Máquina Virtual (VMM), un hipervisor

es una capa de software que reside debajo de las máquinas virtuales y encima del hardware. El hipervisor evita que las máquinas virtuales puedan interactuar directamente con el hardware, en su lugar, maneja las interacciones entre cada máquina virtual y el hardware que todas comparten. De esa manera el aprovechamiento de recursos es asignado de manera ordenada a cada sistema operativo virtual. La figura 9 representa un modelo conceptual de un hipervisor.

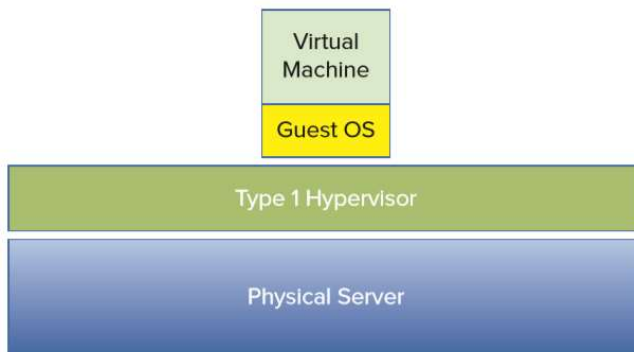


*Figura 9.* Diagrama de Bloques de Hipervisor

Tomada de: Portnoy, 2017, pp. 2

#### 2.8.1.1. Hipervisor tipo 1

El servidor de tipo 1 o “bare-metal” se ejecuta y se instala directamente sobre el hardware, hace las veces de sistema operativo principal. Al comunicarse con el equipo físico de manera inmediata, le resulta más fácil manejar los recursos de hardware, y mejora su eficiencia. Adicionalmente, se evita el gasto innecesario de recursos que se tendría en un sistema operativo convencional. Se lo considera más seguro, debido a que, si un huésped falla, es posible recuperar un estado antes del siniestro, o simplemente se puede eliminar. La figura 10 permite entender conceptualmente lo que representa un hipervisor tipo 1.

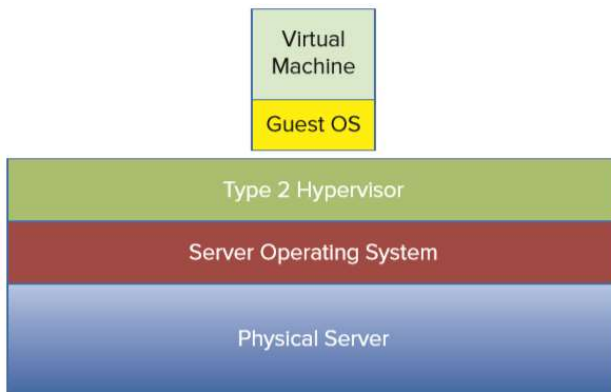


*Figura 10.* Diagrama de Bloques de Hipervisor Tipo 1

Tomada de: Portnoy, 2017, pp. 3

#### 2.8.1.2. Hipervisor tipo 2

Funciona como una aplicación que se ejecuta sobre un sistema operativo tradicional. Utiliza los recursos de administración del sistema operativo local para su beneficio, por lo tanto, es fácil de instalar e implementar; la configuración ya ha sido llevada a cabo en el sistema operativo anfitrión. Resulta útil para una implementación temporal no crítica. Por otro lado, las operaciones requeridas por los sistemas huéspedes, se delegan hacia el sistema operativo anfitrión, lo cual ralentiza el proceso. Además, el riesgo de un fallo general es mayor, debido a que, si el sistema principal del servidor sufre una ruptura, las máquinas virtuales pueden sufrir daños. A continuación, se observa el diagrama de bloques de un hipervisor tipo 2 en la figura 11.



*Figura 11.* Diagrama de Bloques Hipervisor Tipo 2.

Tomada de: Portnoy, 2017, pp. 4

## 2.9. Interfaz de línea de comandos

Una Interfaz de línea de comandos utiliza comandos de texto para introducirlos en un cuadro de texto, que a su vez los interpreta y ejecuta. A pesar de que la mayoría de los usuarios ya no utiliza la línea de comandos para interactuar con los sistemas, los administradores y desarrolladores todavía dan uso de esta interfaz. Esto es debido a que existen herramientas y configuraciones que no son asequibles mediante otro método. (Silverschatz, 2006, p. 35-36). Es posible identificar en la figura 12.

```

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog?
[yes/no]: no

Press RETURN to get started!

Router>ena
Router#

```

*Figura 12.* Captura CLI.

## 2.10. Interfaz gráfica de usuario



Una Interfaz Gráfica de Usuario o GUI, es una interfaz que contiene controles gráficos, tales como ventanas, iconos y botones. En la actualidad, la mayoría de los sistemas son presentados a través de una interfaz gráfica. Aquellos que no se presentan a través de una GUI, utilizan una línea de comandos. (Silverschatz, 2006, p.36-37). Así como se observa la figura 13.

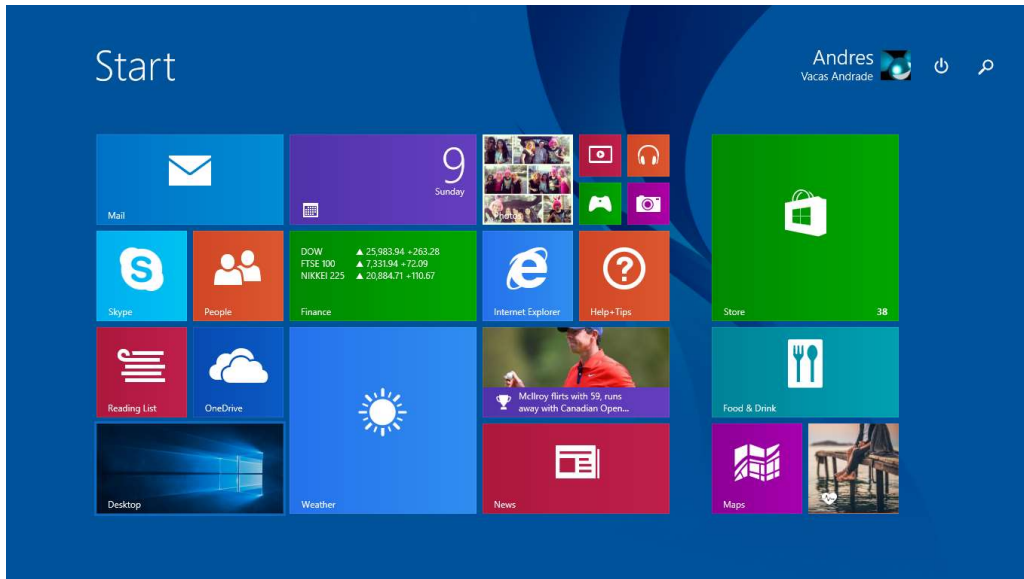


Figura 13. Interfaz Gráfica de Usuario Windows 8.

## 2.11. Microsoft Visual Studio

Es un ambiente de desarrollo integrado de Microsoft, el cual permite la creación, ejecución y depuración de programas y aplicaciones. Estos programas pueden estar desarrollados en distintos lenguajes de programación como: Visual C# o Visual Basic. Tiene bloques de construcción predefinidos, los cuales, mediante el procedimiento de arrastrar y colocar, permiten crear programas de manera sencilla. (Deitel, 2007, pp. 23-25). Se puede identificar una Forma de Windows en la figura 14.

### 2.11.1. Formas de Windows

Un formulario de Windows es una ventana llena de controles, que posibilita crear aplicaciones con interfaces gráficas (GUI). De esa manera le permite al usuario interactuar con un menú sencillo y procesar datos de manera simple. La biblioteca de Windows Forms de Visual Studio permite el diseño de aplicaciones, generando eventos a partir de acciones de los controles.

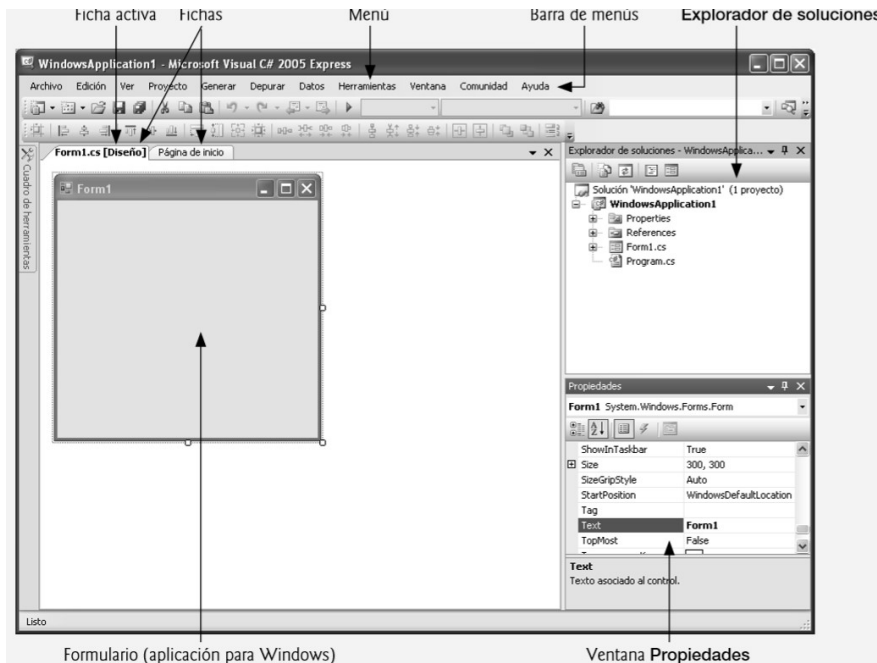


Figura 14. Ventana de Visual Studio

Tomada de: Deitel, 2007, pp. 83

## 2.12. Programación orientada a objetos

Es un tipo de diseño de software, en el cual se tiene muy en cuenta las características de los objetos físicos, para construir una abstracción lógica. Adicionalmente, se consideran las características de los objetos físicos, a las que se denomina atributos. Y también, se declara que los objetos tienen acciones o comportamientos, a los cuales se les denomina métodos. El propósito es asemejar el mundo real con el modelo de software. De esa manera se puede crear un ‘molde’

o clase de un objeto y crear nuevos objetos, los cuales “heredan” las propiedades del objeto creador. (Deitel, 2007, pp. 83-84)

### 2.12.1. Clase

Una clase es una plantilla que posee todos los métodos y atributos de un objeto en particular. Asimismo, un objeto es una instancia de la clase, la cual contiene valores definidos en las variables que componen los atributos. De esa manera, futuros sistemas de software pueden reutilizar esas clases. Obsérvese la figura 15.

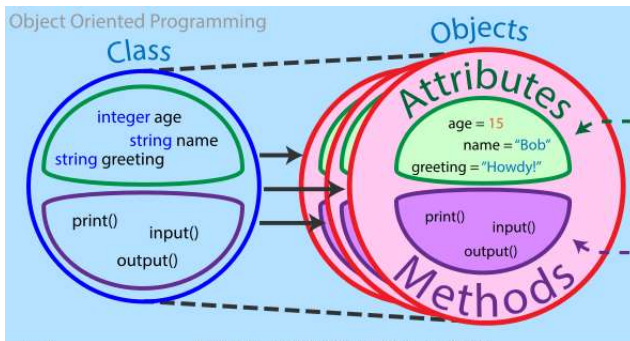


Figura 15. Diagrama de Clase y Objetos.

Recuperada de: Brilliant Org. s.f.

## 3. CAPITULO III: ANÁLISIS CONDICIONES INICIALES

Para el desarrollo del proyecto se utiliza el modelo de proceso de software “Waterfall”. El modelo se denomina Cascada, debido al esquema que mantiene, de una fase a la siguiente. Y debido a su simplicidad, se adapta de manera adecuada al desarrollo del sistema de gestión de redes Cisco. Adicionalmente, el modelo permite la corrección de problemas, a medida que estos sean descubiertos.

El análisis de condiciones iniciales permite la recopilación de los parámetros necesarios para el modelado de las interfaces. Esto posibilita determinar las necesidades del sistema y definir una solución a medida. Dentro del modelo de

cascada, el análisis de condiciones iniciales corresponde a la primera fase, así como se observa en la figura 16 a continuación.

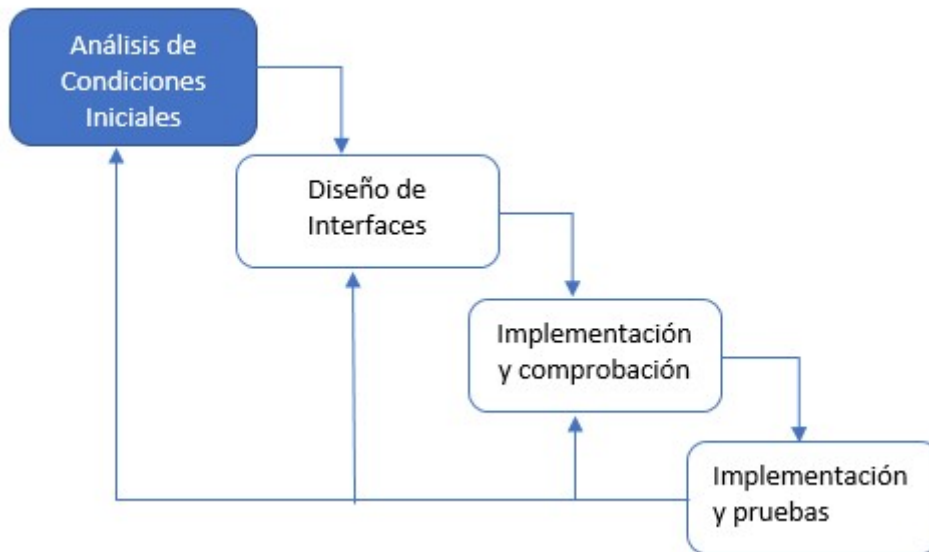


Figura 16. Modelo Cascada, Fase Análisis de Condiciones Iniciales

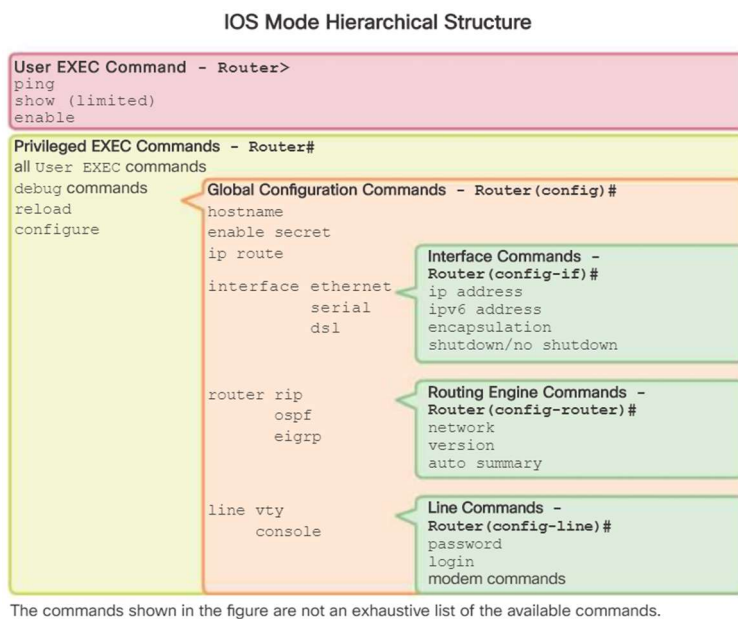
### 3.1. Modos de operación Cisco IOS

El Sistema operativo IOS acomoda las configuraciones del sistema, en una estructura jerárquica compuesta por modos. Cisco indica que las condiciones iniciales para implementación de red, de Conmutadores y Enrutadores Cisco, son similares entre ellas y soportan comandos semejantes (Cisco NetAcad, 2019). Y los modos principales de configuración son:

- Modo User Executive (User EXEC)
- Modo Privileged Executive (Privileged EXEC)
- Modo Global Configuration
- Modos de Configuración específicos. Ej. Interface

Cada modo tiene distintas funcionalidades y su propio conjunto de comandos disponibles para cada modo. Es necesario tener en cuenta que algunas configuraciones afectan a todo el dispositivo o solamente a un componente de este. Por ejemplo, si se ingresa al nivel de configuración de la interfaz Gigabit Ethernet

0/0, los cambios realizados dentro de este nivel afectan solamente a la interfaz Gigabit 0/0. Es posible utilizar la Estructura Jerárquica de Modos IOS para lograr la organización de los comandos dentro del sistema. Se observa la jerarquía en la figura 17.



*Figura 17.* Modelo de Estructura Jerárquica de Modos de IOS.

Tomada de: NetAcad s.f.

### 3.2. Estructura de comandos IOS

Cada comando tiene su propio formato de argumentos que recibe, pero en general la sintaxis que existe para los comandos de Cisco IOS, es similar. Se tiene el comando, seguido de un espacio y luego los argumentos. Los comandos ejecutan las acciones y los argumentos definen la información de ingreso. El "Prompt" es el texto de entrada, este define el modo de operación en el que se encuentra la línea de comandos. Finalmente, para ejecutar el comando ingresado, se presiona la tecla [enter]. La computadora interpreta la acción como un salto de línea "\r\n". En la figura 18, se observa, en síntesis, la sintaxis de los comandos del sistema IOS.

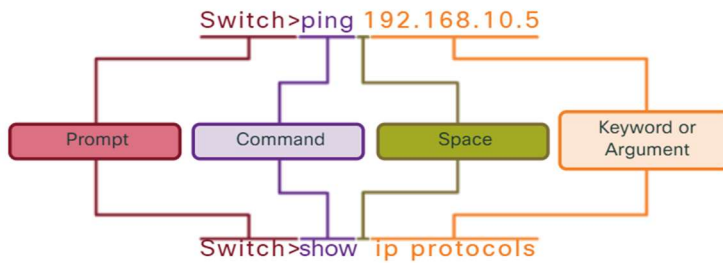


Figura 18. Diagrama de Sintaxis de Comandos IOS

Tomada de: Netacad s.f.

### 3.3. Análisis enrutador

#### 3.3.1. Configuraciones iniciales

Cisco recomienda que inicialmente se deben completar las siguientes configuraciones iniciales: el nombre del equipo, el "banner MOTD" (mensaje del día), habilitación de búsqueda de DNS, mínimo de caracteres para clave User EXEC y el dominio correspondiente. (Cisco NetAcad, 2019). En la tabla 1, se observa la jerarquía de los modos y los comandos necesarios para llevar a cabo las configuraciones anteriormente mencionadas.

Tabla 1. Configuraciones Iniciales de Enrutador

User EXEC > Enable
Privileged EXEC # Configure terminal
Global Configuration (config)# <ul style="list-style-type: none"> <li>• Hostname <b>nombreEquipo</b></li> <li>• Banner motd <b>#mensajeDelDia#</b></li> <li>• No ip domain-lookup</li> <li>• Security passwords min-lenght <b>longitud</b></li> <li>• Ip domain-name <b>dominio</b></li> </ul>

### 3.3.2. Configuraciones de interfaces LAN

Son las configuraciones relacionadas con las interfaces de red del enrutador. Con el propósito de poder establecer comunicación con las interfaces, se debe configurar una dirección de IP y su respectiva máscara. Por defecto las interfaces no están activadas, así que es necesario hacerlo. Es posible también, establecer una leve descripción de la interfaz, con el propósito de identificarla fácilmente. Se observan los comandos en la tabla 2.

Tabla 2. Configuración de Interfaz de Red de Enrutador

User EXEC-> <b>Enable</b>	
Privileged EXEC-# <b>Configure terminal</b>	
Global Configuration-(config)#	
Interface <b>interfaz</b>	Interface Commands – (config-if) # <ul style="list-style-type: none"> <li>• Ip address <b>direccionIP</b> <b>mascara</b></li> <li>• No shutdown</li> <li>• Description <b>descripción</b></li> </ul>

### 3.3.3. Configuraciones de seguridad

Cisco recomienda limitar el acceso a los dispositivos de red, colocándolos en closets y racks asegurados, evitando así intervención de personal no autorizado. A pesar de ello, el acceso puede ocurrir a través de la red, por lo que es necesario configurar contraseñas que limitan el acceso. Es adecuado también, utilizar contraseñas con una buena cantidad de caracteres variados. Existen distintos niveles de acceso, dependiendo de la jerarquía del modo:

- Enable password – Limita el acceso al modo “privileged EXEC”.

- Enable secret – Limita el acceso al modo “privileged EXEC” de manera cifrada
- Console Password – Limita el acceso usando comunicación de consola
- VTY password – Limita el acceso sobre Telnet.

### 3.3.3.1. Configuraciones de acceso EXEC privilegiado

El puerto de consola debe estar protegido con una clave, con la finalidad de evitar que un usuario no autorizado conecte directamente con el dispositivo y obtenga acceso. Además, en caso de que alguien, en efecto, acceda a los archivos de configuración, estos deben estar cifrados para que no puedan ser descubiertos. En la tabla 3, de configuraciones a continuación, se establece como llevar a cabo lo mencionado anteriormente.

Tabla 3 Configuraciones de Acceso EXEC Privilegiado de Enrutador

User EXEC-> <b>Enable</b>
Privileged EXEC-# <b>Configure terminal</b>
Global Configuration-(config)# <ul style="list-style-type: none"> <li>• Enable secret <b>contraseña</b></li> </ul>

### 3.3.3.2. Configuraciones de líneas VTY

Estas líneas permiten el acceso a los dispositivos Cisco a través de Telnet y SSH. La mayoría de los dispositivos utilizan hasta 16 líneas VTY, numeradas del 0 al 15. Se puede utilizar la misma contraseña para todas las conexiones, a pesar de ello, es recomendable utilizar diferentes contraseñas. En la tabla 4, a continuación, se indican las configuraciones de líneas VTY para operar con SSH.



Tabla 4. Configuraciones de Líneas VTY de Enrutador

User EXEC-> <b>Enable</b>	
Privileged EXEC-# <b>Configure terminal</b>	
Global Configuration-(config)#	
Line vty <b>0 15</b>	Line Commands – (config-line) # <ul style="list-style-type: none"> <li>• Login local</li> <li>• Transport input ssh</li> </ul>

### 3.3.4. Configuraciones SSH

Es necesario habilitar SSH en un enrutador cisco si se requiere acceder por este medio. Para hacerlo, es necesario configurar el nombre del equipo, el nombre del dominio al cual pertenece y la información de autenticación. Es también necesario generar llaves RSA, como mínimo con 1024 bits, para admitir SSH versión 2. Se observa en la Tabla 5.

Tabla 5. Configuraciones SSH de Enrutador

User EXEC-> <b>Enable</b>	
Privileged EXEC-# <b>Configure terminal</b>	
Global Configuration-(config)# <ul style="list-style-type: none"> <li>• Hostname nombreEquipo</li> <li>• Ip domain-name <b>dominio</b></li> </ul>	

<ul style="list-style-type: none"> <li>• crypto key generate rsa: <b>1024</b></li> <li>• username <b>usuario</b> secret <b>contraseña</b></li> <li>• enable secret <b>clave</b></li> </ul>	
Line vty <b>0 15</b>	Line Commands – (config-line) # <ul style="list-style-type: none"> <li>• Login local</li> <li>• Transport input ssh</li> <li>• ip ssh version 2</li> </ul>

### 3.3.5. Configuraciones de enrutamiento RIP

RIP es uno de los protocolos de enrutamiento dinámico, más básicos que existen. Permite la conectividad entre los tramos de red conectados a los enrutadores. Para configurar es necesario establecer si se utiliza la versión RIP 1 o 2. Se indican las redes implicadas sin máscara. Si se resumen las redes y las interfaces pasivas, por donde no se difunden las rutas. En la tabla 6 se indican las configuraciones necesarias.

Tabla 6. Configuraciones de Enrutamiento RIP

User EXEC-> <b>Enable</b>	
Privileged EXEC-# <b>Configure terminal</b>	
Global Configuration-(config)#	
<b>Router rip</b>	Router Commands –(config-router) # <ul style="list-style-type: none"> <li>• Version <b>1 o 2</b></li> <li>• Network <b>redesImplicadas</b></li> <li>• <b>No</b> Auto-summary</li> <li>• Passive interface <b>interfaz</b></li> <li>• Default-information originate</li> </ul>

### 3.3.6. Configuraciones de servidor DHCP

Los enrutadores Cisco con sistema operativo IOS pueden, a menudo, configurarse para funcionar como servidor DHCP. Las direcciones que es capaz de asignar un dispositivo con IOS son de versión IPv4. Inicialmente, se excluyen las direcciones que se conoce, son utilizadas por otros dispositivos. Se configura el pool, es decir el grupo de DHCP y se le asigna un nombre. Por último, se asigna la información que se requiere que el servidor propague: portal por defecto, servidor DNS, red, entre otros. Se indica la configuración en la tabla 7.

Tabla 7. Configuraciones de Servidor DHCP

User EXEC-> <b>Enable</b>	
Privileged EXEC-# <b>Configure terminal</b>	
Global Configuration-(config)# <ul style="list-style-type: none"> <li>• Service dhcp</li> <li>• Ip dhcp excluded-address <b>dirección</b></li> </ul>	
Ip dhcp pool <b>Name</b>	DHCP Commands –(dhcp-config) # <ul style="list-style-type: none"> <li>• Default-router <b>ipRouter</b></li> <li>• Network <b>red máscara</b></li> <li>• Dns-server <b>ipDNS</b></li> <li>• Lease <b>díasValidos</b></li> </ul>

### 3.3.7. Configuraciones de subinterfaces

Se divide la interfaz física en varias interfaces lógicas. Normalmente se utiliza para conectar varias VLANs entre sí, utilizando encapsulación 802.1Q. Tiene las mismas variables que una interfaz física. Por lo que se configura de manera similar, como puede apreciarse en la tabla 8, a continuación:

Tabla 8. Configuraciones de Subinterfaces de Enrutador

User EXEC-> <b>Enable</b>	
Privileged EXEC-# <b>Configure terminal</b>	
Global Configuration-(config)#	
Interface <b>interfaz</b>	Interface Commands – (config-subif) # <ul style="list-style-type: none"> <li>• Encapsulation dot1Q <b>IdVLAN</b></li> <li>• Ip address <b>direccionIP</b> <b>máscara</b></li> <li>• No shutdown</li> <li>• Description <b>descripción</b></li> </ul>

### 3.4. Análisis conmutador

#### 3.4.1. Configuraciones iniciales

La modalidad en la cual se configura un conmutador se asemeja bastante a las configuraciones de un enrutador. Por lo tanto, los parámetros de configuración que se le asignan al “switch” son prácticamente los mismos. Un nombre de equipo, una dirección IP asignada a una interfaz y configuraciones de seguridad. (Tabla 9).

Tabla 9. Configuraciones Iniciales de Conmutador

User EXEC > Enable
-----------------------

Privileged EXEC # Configure terminal
Global Configuration (config)# <ul style="list-style-type: none"> <li>• Hostname <b>nombreEquipo</b></li> <li>• Banner motd <b>#mensajeDelDia#</b></li> <li>• No ip domain-lookup</li> <li>• Security passwords min-lenght <b>longitud</b></li> <li>• Ip domain-name <b>dominio</b></li> </ul>

### 3.4.2. Configuraciones de interfaz de manejo

Con el objeto de configurar el conmutador para acceso remoto, es necesario configurarlo con una dirección IP y una debida máscara. Así también, debe estar configurado con un default Gateway, para ser configurado de manera remota. La IP en los “Switches” Cisco no se asigna a una interfaz física, sino a una interfaz virtual (SVI). La SVI está asociada con una VLAN. Se recomienda que la VLAN de administración sea distinta a la VLAN 1, por lo cual se genera una VLAN 99. Por último, se asignan puertos a la VLAN en modo de acceso y así poder acceder a la interfaz de administración (SVI). Se observa la configuración en la tabla 10.

Tabla 10. Configuraciones de Interfaz de Manejo de Conmutador

User EXEC > Enable
Privileged EXEC-# <b>Configure terminal</b>
Global Configuration-(config)# <ul style="list-style-type: none"> <li>• Ip default-gateway <b>IPPuertoSalida</b></li> </ul>

VLAN <b>IdVLAN</b>	VLAN Commands – (config-vlan) # <ul style="list-style-type: none"> <li>Name <b>nombreVLAN</b></li> </ul>
Interface VLAN <b>IdVLAN</b>	Interface Commands – (config-if)# <ul style="list-style-type: none"> <li>Ip address <b>direccionIP</b> <b>máscara</b></li> <li>No shutdown</li> <li>Description <b>descripción</b></li> </ul>
Interface <b>Interfaz</b>	Interface Commands – (config-if)# <ul style="list-style-type: none"> <li>Switchport mode <b>access</b></li> <li>Switchport access vlan <b>IdVLAN</b></li> </ul>

### 3.4.3. Configuraciones SSH

De igual manera, es necesario habilitar SSH en el conmutador si se requiere acceder por este medio. Para hacerlo, es necesario configurar el nombre del equipo, el nombre del dominio al cual pertenece y la información de autenticación. Es también necesario generar llaves RSA, como mínimo con 1024 bits, para admitir SSH versión 2. Se genera una clave para el modo “Privileged EXEC” y una contraseña para las líneas VTY 0 – 15. Los comandos necesarios, así como la jerarquía de los modos, puede observarse en la tabla 11.

Tabla 11. Configuraciones SHH de Conmutador

User EXEC-> <b>Enable</b>
Privileged EXEC-# <b>Configure terminal</b>

Global Configuration-(config)#	
<ul style="list-style-type: none"> <li>• Hostname nombreEquipo</li> <li>• Ip domain-name <b>dominio</b></li> <li>• crypto key generate rsa: <b>1024</b></li> <li>• username <b>usuario</b> secret <b>contraseña</b></li> <li>• enable secret <b>clave</b></li> </ul>	
Line vty	Line Commands – (config-line) #
<b>0 15</b>	<ul style="list-style-type: none"> <li>• Login local</li> <li>• Transport input ssh</li> <li>• ip ssh version 2</li> </ul>

#### 3.4.4. Configuraciones VLAN

Las configuraciones VLAN se almacenan sobre la memoria flash, por lo cual no es necesario ejecutar el comando “copy running-config” para guardar las configuraciones VLAN. Se indica un identificador de VLAN, que es un numero desde 1 hasta 4096 y un nombre para dicha VLAN. Luego para poder configurar la interfaz virtual, correspondiente a dicha VLAN, se asigna una dirección IP con su respectiva mascara y una descripción. Se observa en la tabla número 12.

Tabla 12. Configuraciones de VLAN

User EXEC > Enable
Privileged EXEC-# <b>Configure terminal</b>
Global Configuration-(config)#

VLAN <b>IdVLAN</b>	VLAN Commands – (config-vlan) # <ul style="list-style-type: none"> <li>Name <b>nombreVLAN</b></li> </ul>
Interface VLAN <b>IdVLAN</b>	Interface Commands – (config-if)# <ul style="list-style-type: none"> <li>Ip address <b>direccionIP</b> <b>máscara</b></li> <li>No shutdown</li> <li>Description <b>descripción</b></li> </ul>

### 3.4.5. Configuraciones puerto troncal y acceso

Con el propósito de admitir el acceso de puertos requeridos a una VLAN, es imprescindible asignarlos como puertos de acceso y asociarlos con dicha VLAN. Para lograrlo, simplemente se declaran los puertos como puertos de acceso y luego se asigna la VLAN correspondiente, así como es posible observar en la tabla 13.

Tabla 13. Configuraciones de Puerto de Acceso

User EXEC > Enable	
Privileged EXEC-# <b>Configure terminal</b>	
Global Configuration-(config)#	
Interface-range <b>Interfaz</b>	Interface Commands – (config-if)# <ul style="list-style-type: none"> <li>Switchport mode <b>access</b></li> <li>Switchport access vlan <b>IdVLAN</b></li> </ul>



Los enlaces troncales se establecen entre dos conmutadores y permiten que el tráfico de varias VLANs sea conducido. Para configurar puertos troncales, simplemente se le indica al puerto, que es un puerto troncalizado. También, se debe indicar las VLANs que están permitidas. Es posible agregar una VLAN nativa. (Tabla 14).

Tabla 14. Configuraciones de Puerto Troncal

User EXEC > Enable	
Privileged EXEC-# <b>Configure terminal</b>	
Global Configuration-(config)#	
Interface-range <b>Interfaz</b>	Interface Commands – (config-if)# <ul style="list-style-type: none"> <li>• Switchport mode <b>trunk</b></li> <li>• Switchport trunk allowed vlan <b>IdVLAN</b></li> <li>• Switchport trunk native vlan <b>IdVLAN</b></li> </ul>

#### 3.4.6. Seguridad de Puertos

Se recomienda la configuración de puertos de seguridad, sobre todo si se implementa en un medio de producción. “Port security” limita el número de direcciones MAC validas en un puerto. Si el número de direcciones MAC admitidas excede la cantidad configurada, se genera una violación de seguridad. La interfaz por configurar como port security, debe estar habilitada en modo “access”. Se puede identificar lo anteriormente mencionado en la tabla 15.

Tabla 15. Configuraciones de Seguridad de Puertos

User EXEC > Enable	
Privileged EXEC-# <b>Configure terminal</b>	
Global Configuration-(config)#	
Interface-range <b>Interfaz</b>	Interface Commands – (config-if)#  <ul style="list-style-type: none"> <li>• Switchport mode <b>access</b></li> <li>• Switchport port-security maximum <b>numeroMaximo</b></li> <li>• Switchport port-security violation {<b>restrict/shutdown</b>}</li> </ul>

#### 4. CAPITULO IV: DISEÑO DE INTERFACES

En la etapa de diseño de interfaces, se utiliza la información recolectada en la fase de análisis de condiciones iniciales, con el fin de diseñar el sistema. Adicionalmente se aprovecha para ensayar las funcionalidades de cada módulo de manera independiente en la fase de: Implementación y comprobación. Es posible observar en la figura 19 las fases correspondientes resaltadas en azul.

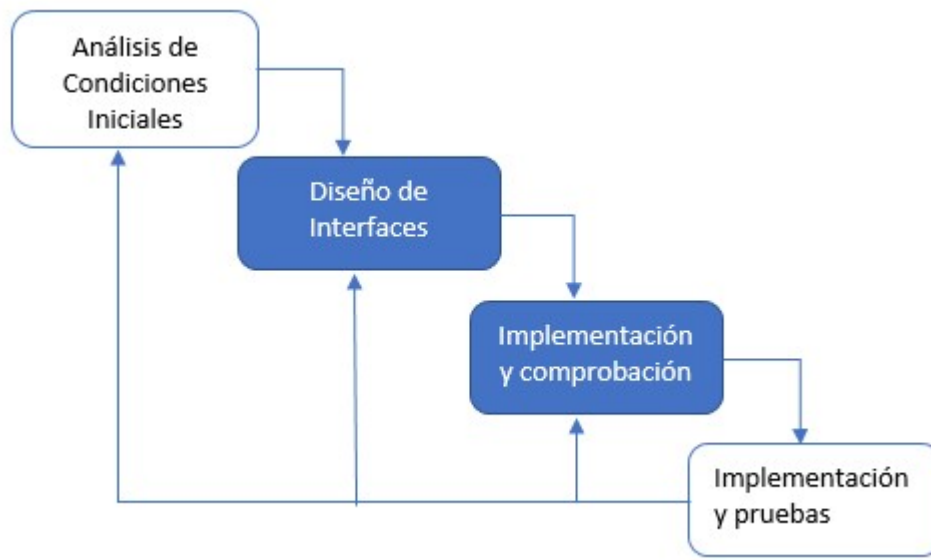


Figura 19. Modelo Cascada

#### 4.1. Terminal serial

La funcionalidad del programa empieza con una herramienta adicional, una sencilla interfaz, que establece una conexión serial con el dispositivo de red Cisco. En el control de caja de combo, aparecen los puertos seriales, donde se selecciona el correspondiente equipo de red. Utilizando el botón [Connect], se efectúa la conexión con el equipo seleccionado. Los comandos se ingresan en el cuadro de texto correspondiente, en la parte inferior. Mientras que, en la ventana superior, se lee la respuesta del dispositivo conectado. Adicionalmente, en el texto "Status", se observa el estado de la conexión. Es posible observar la interfaz en la figura 20.

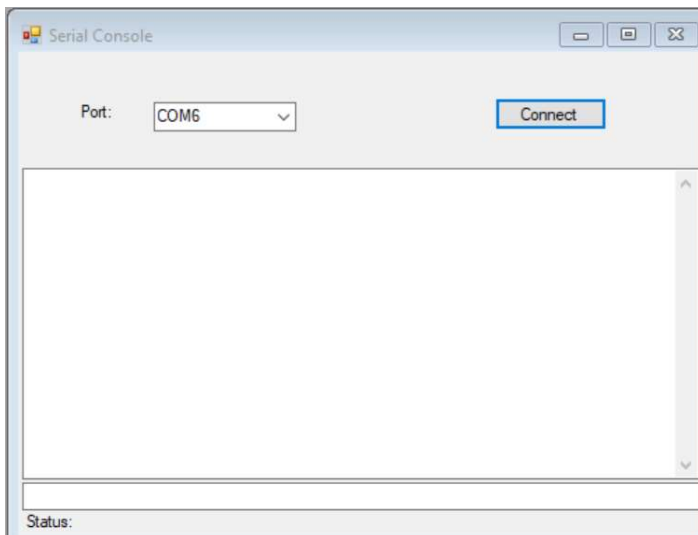


Figura 20. Ventana Terminal Serial.

## 4.2. Terminal SSH

Se diseña una interfaz simple, la cual tiene la función de establecer una sesión SSH. En ella se indica: la dirección IP del destino, el puerto que se utiliza para el protocolo SSH. Además, accede información de autenticación: usuario y contraseña. Y mediante la activación del botón [Connect], se inicia el proceso de generar una sesión SSH utilizando la información ingresada. Es posible observar la interfaz en la figura 21.

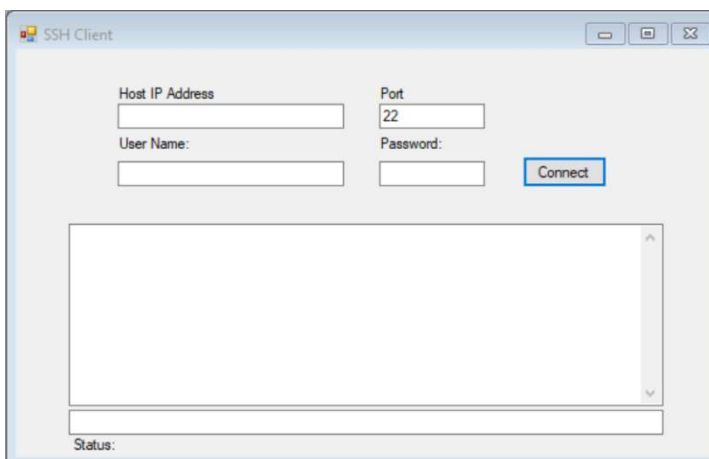


Figura 21. Ventana Terminal SSH.

En el caso de ser errónea la información de autenticación, se indica el resultado en un dialogo, así como se observa en la Figura 22.

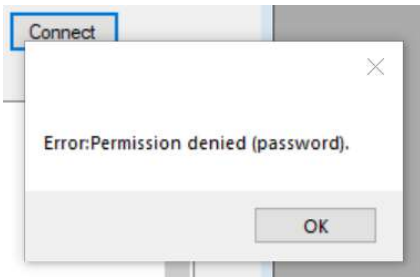


Figura 22. Dialogo de Permiso Denegado.

### 4.3. Diseño de interfaces de enrutador

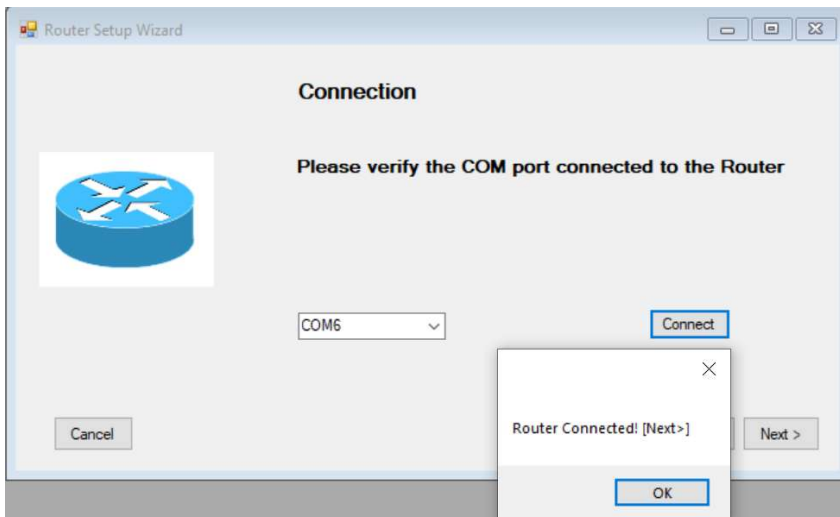
#### 4.3.1. Agente de agregación

Para establecer una conexión SSH con un dispositivo Cisco, es mandatorio tener una dirección IP asignada a una interfaz. Además de credenciales para líneas VTY y servicio de SSH habilitado. Por ello, el Agente de Inicio dispone de una interfaz que le indica al usuario cómo conectar un dispositivo mediante un cable serial o USB. Para continuar se selecciona el botón [Next >]. Se puede observar en la figura 23 a continuación:



Figura 23. Pantalla de Bienvenida.

Luego, el agente solicita al usuario identificar el puerto serial que se utiliza para la comunicación. Al dar clic en conectar, si la condición es apropiada, un dialogo indica que es posible continuar con la siguiente ventana. El botón [Next>] comunica con la siguiente forma. Como es posible observar en la Figura 24.



*Figura 24.* Pantalla de Conexión.

En la siguiente ventana, la ventana de configuración de red permite ingresar parámetros necesarios para la conectividad. En sus campos, es posible indicar: La interfaz, la dirección IP para esa interfaz, la máscara correspondiente a la IP y una ligera descripción de la interfaz. En esta ventana, es posible configurar varias interfaces, solamente se selecciona las distintas interfaces, de la caja de combo y se presiona en el botón [Configure]. La figura 25 permite visualizar la interfaz diseñada.

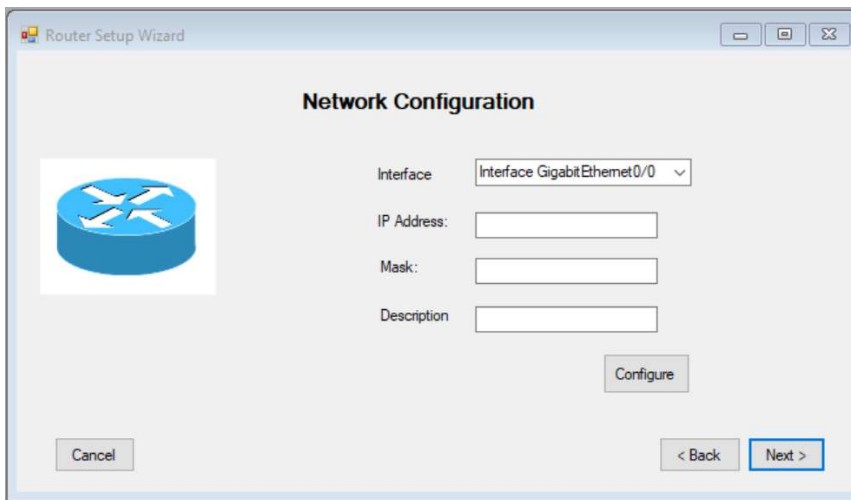


Figura 25. Pantalla de Parámetros de Red

En la ventana a continuación, existen campos para agregar información necesaria para habilitar SSH. Por ejemplo, el nombre del equipo, el dominio, el nombre de usuario, contraseña de líneas VTY y clave de "User EXEC". Al indicar el botón [Configure], se llevan a cabo la asignación de los valores. Es posible observar la Figura 26.

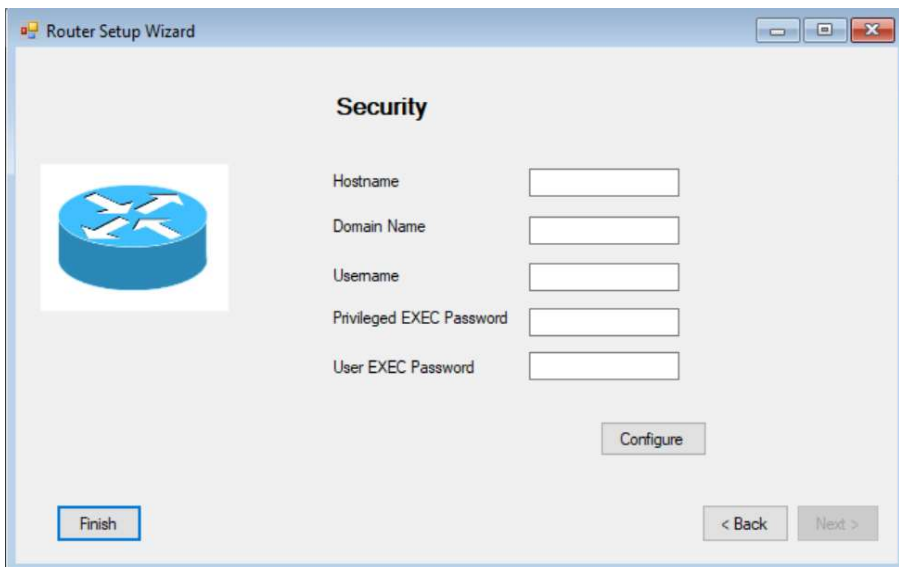


Figura 26. Pantalla de Parámetros de Seguridad.

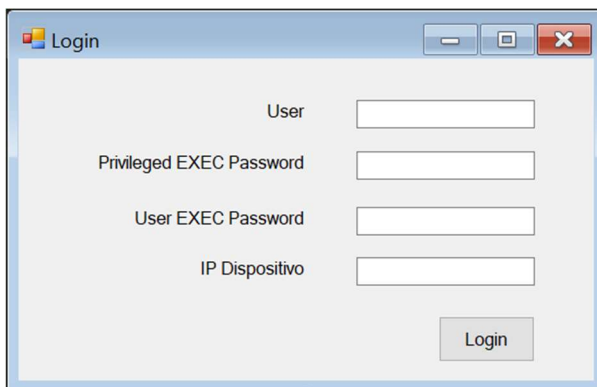
Una vez terminado el proceso de adicción, se activa el botón [Finish], el mismo que cierra la forma. Ahora ya es posible proseguir al agente de configuración.

### 4.3.2. Agente de configuración

El agente de configuración permite establecer las variables correspondientes para permitir la conectividad en los enrutadores de la red. Mientras sea posible establecer una sesión SSH, el agente de configuración puede funcionar.

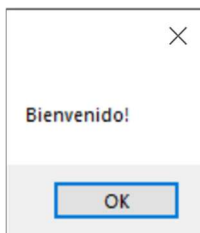
#### 4.3.2.1. Inicio de sesión

Inicialmente es necesario establecer un enlace con el dispositivo, por lo cual se requiere una pantalla de verificación de credenciales, un “Log In” por así decirlo. El mismo que valide la información ingresada por el usuario y la información almacenada en el dispositivo al que se pretende conectar. Para ello se propone la siguiente disposición de controles. Se puede observar en la figura 27.

A screenshot of a Windows-style dialog box titled "Login". The dialog box has a standard title bar with minimize, maximize, and close buttons. Inside the dialog, there are four input fields arranged vertically. The labels for these fields are "User", "Privileged EXEC Password", "User EXEC Password", and "IP Dispositivo". Below the input fields is a "Login" button.

*Figura 27.* Ventana de Inicio de Sesión.

Una vez validado, aparece una pantalla que indica el éxito del ingreso, se observa la figura 28

A screenshot of a small dialog box with a close button (X) in the top right corner. The text inside the dialog box says "Bienvenido!". At the bottom of the dialog box is an "OK" button.

*Figura 28.* Ventana de Acceso Verificado.

Caso contrario, se da un mensaje de error, similar al que se puede observar en la Figura 29.



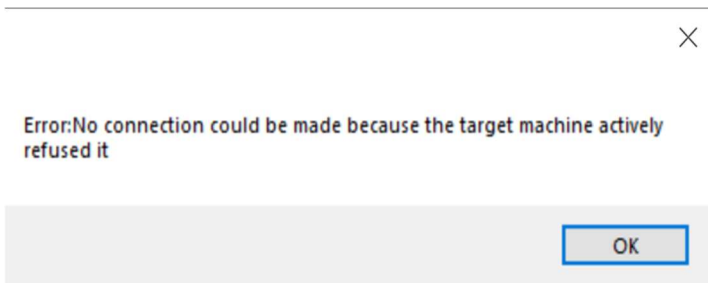


Figura 29. Ventana de Acceso Denegado.

#### 4.3.2.2. Pantalla de configuración

La pantalla de configuración padre presenta una estructura de nodos, basada en la jerarquía de los comandos de los dispositivos con sistema operativo Cisco IOS. El control utilizado es un “TreeView”, el mismo que permite desplegar de manera ordenada las diferentes opciones de configuración del dispositivo, en función del nivel en que se encuentren. Las pantallas de las distintas configuraciones aparecen en el panel de la derecha, a medida que se seleccionan. Se aprecia en la figura 30.

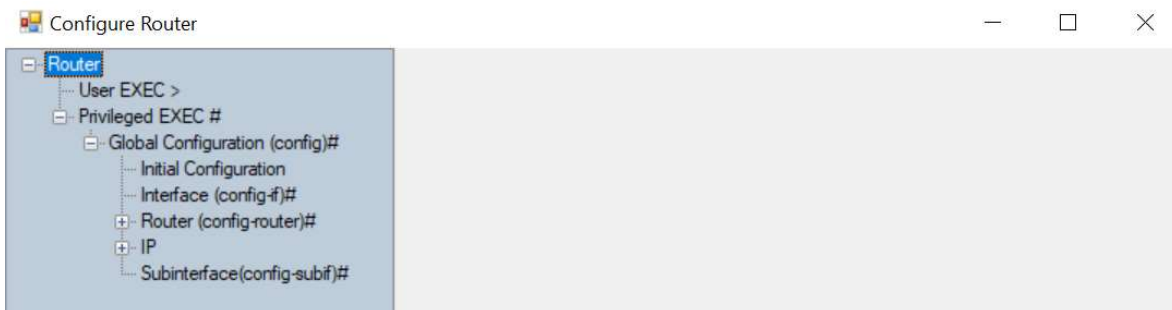


Figura 30. Ventana de Configuración General

##### 4.3.2.2.1. Configuración Inicial

Las variables de configuración inicial incluyen, el nombre del dispositivo, el dominio en el cual se encuentra, si se desea búsqueda de DNS, el mínimo número de caracteres para contraseñas y un mensaje de alerta en caso de acceso no autorizado. Se puede identificar en la figura 31.

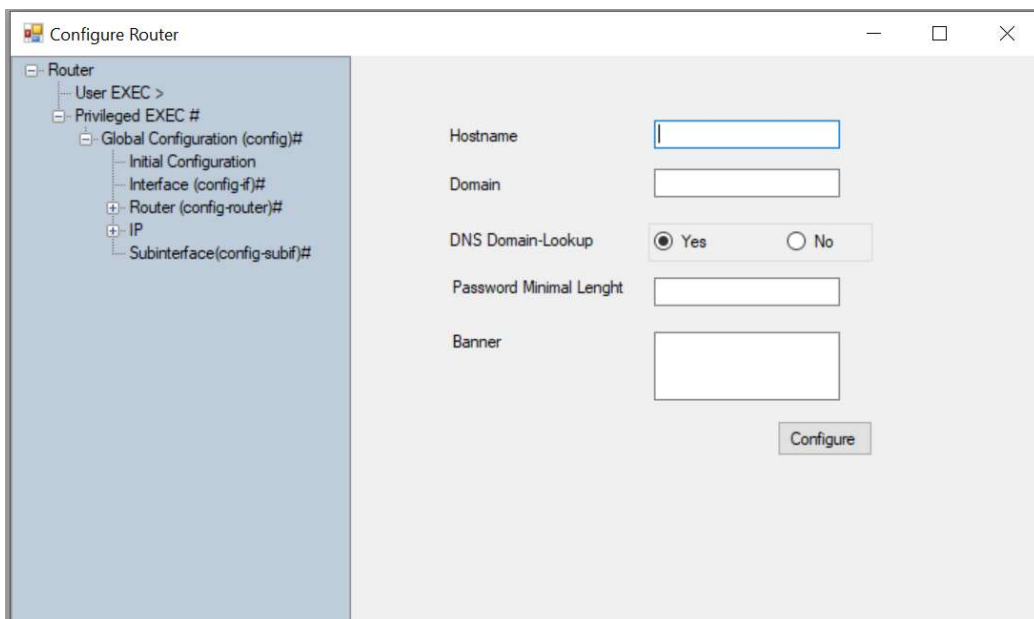


Figura 31. Ventana de Configuración Inicial

#### 4.3.2.2.2. Configuración de interfaces

En la ventana a continuación, que se observa en la figura 32, se configuran los parámetros de red para determinadas interfaces. Se indica la dirección IP, la máscara de la IP, si se enciende o no la interfaz y una leve descripción. El botón [configure], admite llevar a cabo las acciones.

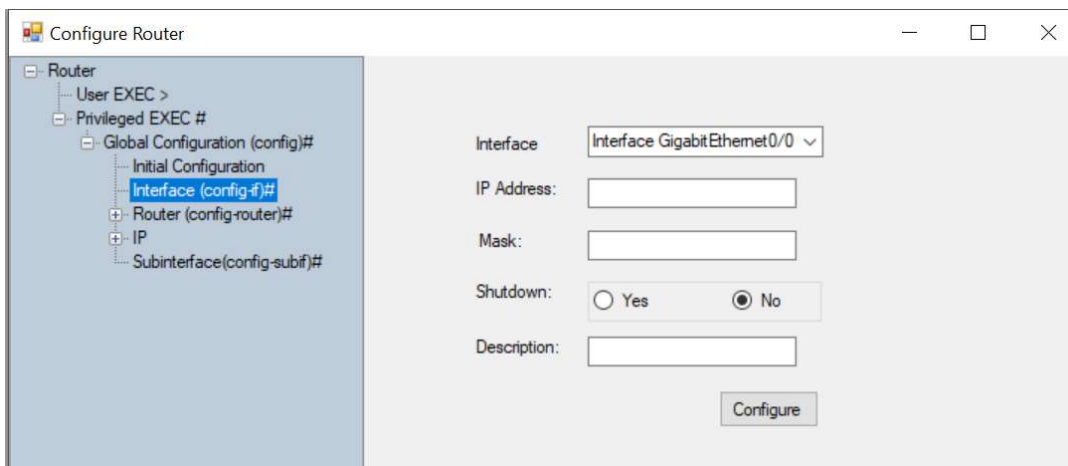


Figura 32. Ventana de Configuración de Interfaz.

#### 4.3.2.2.3. Configuración de enrutamiento RIP

El agente de es capaz de agregar información de enrutamiento al dispositivo enrutador. Las opciones permiten escoger entre enrutamiento con RIP versión 1 o versión 2. Para agregar una red, se ingresa la dirección en la caja de texto correspondiente y al presionar el botón azul [+] se despliegan las redes ingresada debajo. Para borrar las redes, con el botón rojo [X]. Además, es posible indicar la activación de auto resumen de las redes o no. La interfaz pasiva y si se requiere originar información por defecto. Es posible verificar en la figura 33 a continuación:

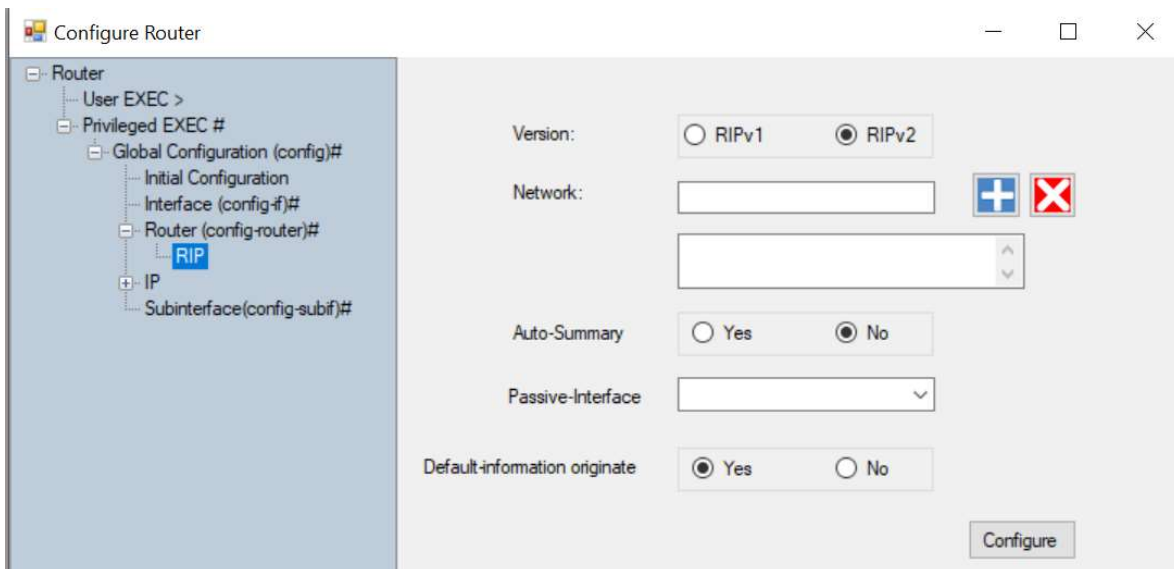


Figura 33. Ventana de Configuración de RIP.

#### 4.3.2.2.4. Configuración de DHCP

La ventana de configuración de servidor DHCP, permite agregar varios “pools” de DHCP, debido a que, si se utiliza VLANs, es necesario asignar diferentes direcciones. Por esto, se agrega el botón [Clear], el mismo que despeja la información de los campos, con el objeto de seguir agregando otro grupo de DHCP. Adicionalmente, se puede activar o desactivar el servicio. La información que se difunde sobre los dispositivos de la red incluye: La ruta de salida por defecto, la red y la máscara del grupo DHCP, el servidor DNS y por último se indica cuanto tiempo en días dura la asignación del servidor. Es posible observar más en detalle en la Figura 34.

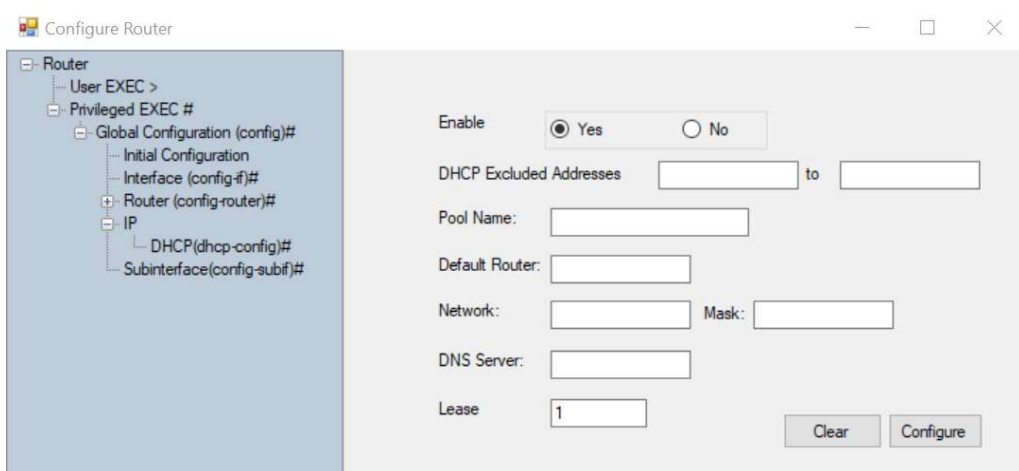


Figura 34. Ventana de Configuración de DHCP.

#### 4.3.2.2.5. Configuración de subinterfaces

Con el propósito de establecer comunicación Inter - VLAN, es necesario configurar subinterfaces con encapsulamiento 802.1Q. Asignar el identificador de VLAN correspondiente a esa subinterfaz y asignar las configuraciones de red correspondientes: Dirección IP, máscara de la IP y descripción de la subinterfaz. La forma que se puede observar en la figura 35 brinda cabida para poder introducir todos estos campos.

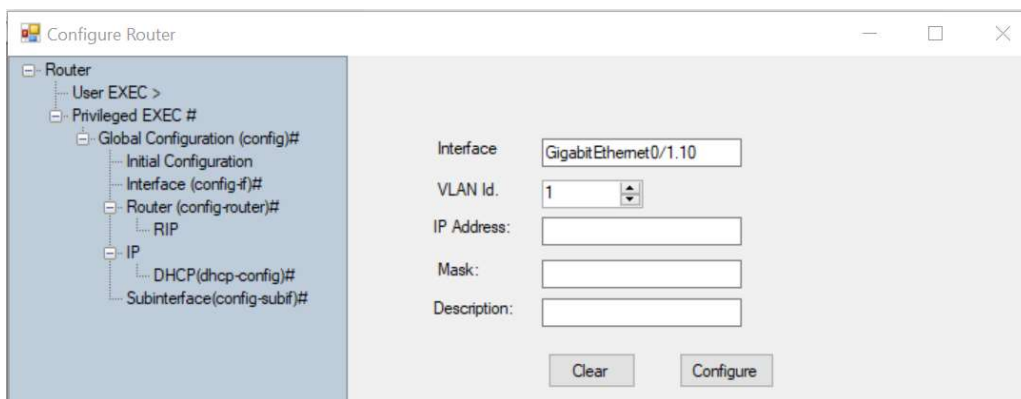


Figura 35. Ventana de Configuración de Subinterfaces.

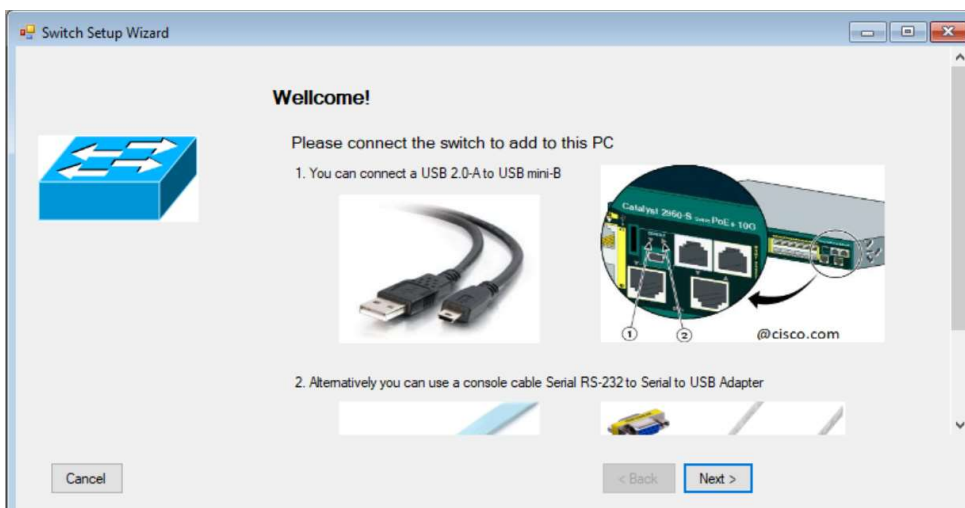
## 4.4. Diseño de interfaces de conmutador

A pesar de que, las configuraciones de “Router” y “Switch” son muy similares, al

momento de asignar atributos de red a las interfaces, existen algunas diferencias. En un enrutador, los parámetros de red se configuran directamente en la interfaz física. Mientras que, en un conmutador, las configuraciones de red se deben configurar sobre una interfaz virtual. Es por esto, que se crean distintos agentes para ambos dispositivos.

#### 4.4.1. Agente de agregación

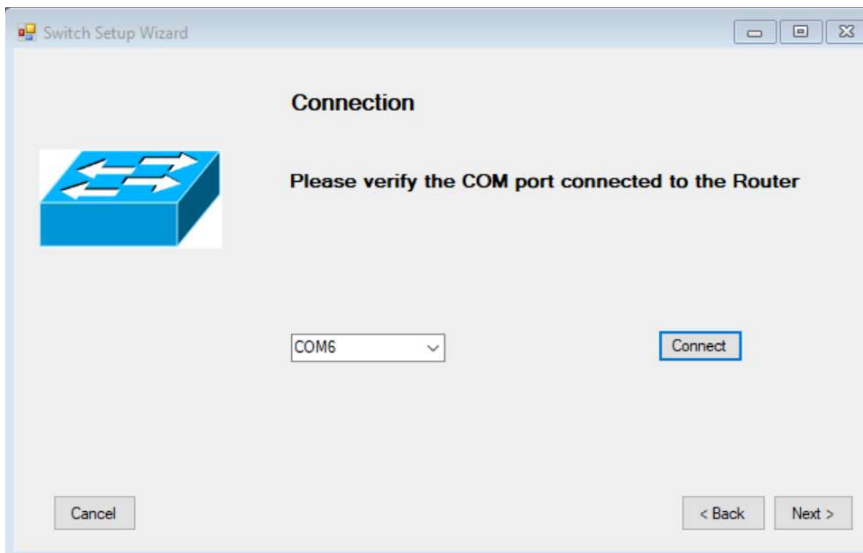
De igual manera, el agente de agregación del conmutador permite “anclar” el dispositivo, al sistema de configuración y monitoreo. Para iniciarlo, la pestaña de Dispositivos> Switch > Agregar Switch, despliega una ventana de instrucciones, la cual le indica al usuario cómo conectar su dispositivo. Indica que se puede utilizar un cable USB o un cable serial RS-232 al puerto de consola y luego al ordenador desde donde se está administrando el sistema. Así como se puede observar en la *Figura 36*, a continuación:



*Figura 36.* Pantalla de Bienvenida.

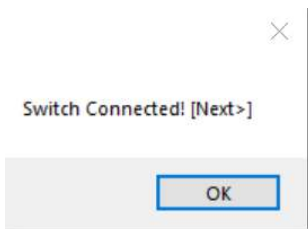
Una vez seleccionado el botón [Next >], se manifiesta una ventana. Esta es la ventana de conexión, la cual permite establecer el puerto serial que se utiliza para conectarse con el dispositivo en cuestión. Al hacer clic en el botón de conectar, se

selecciona el puerto que se despliega en la caja de combo. Así como se evidencia en la figura 37.



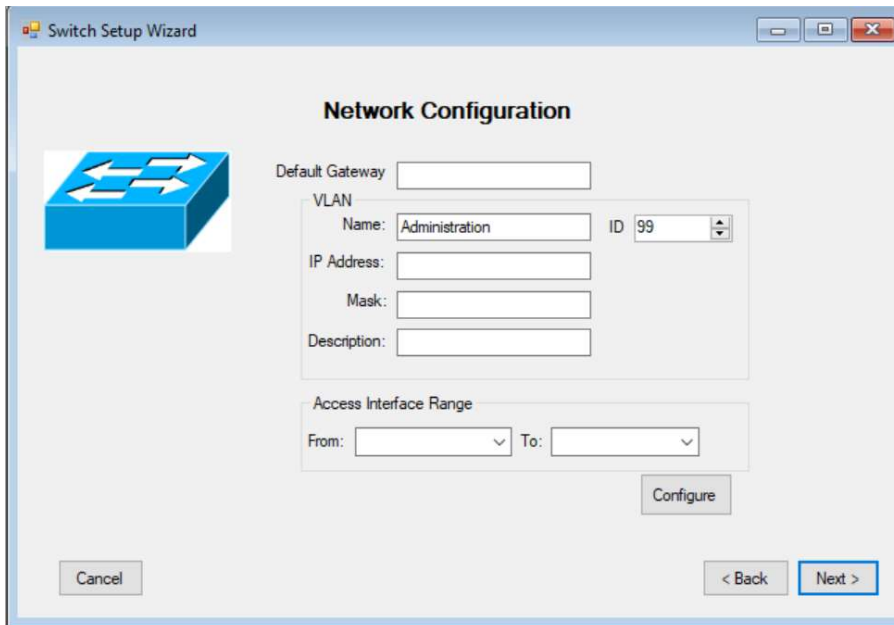
*Figura 37.* Pantalla de Conexión Serial

Se indica que se ha efectuado la conexión de manera exitosa, desplegando un dialogo de tipo "Message Box". Luego, ya es posible continuar con la siguiente ventana escogiendo el botón. Se observa la figura 38.



*Figura 38.* Dialogo de Verificación.

En la ventana que se puede observar a continuación en la figura 39, es posible especificar los detalles necesarios para establecer una comunicación con el dispositivo switch a través de la red. Debido que la interfaz para administración en un switch es virtual, se crea una VLAN u luego se le asigna una interfaz virtual, con la respectiva información. Además, en el cuadro de grupo, se permite establecer cuales han de ser las interfaces físicas de acceso a esta VLAN. Con el botón [Configure] se llevan a cabo las acciones.



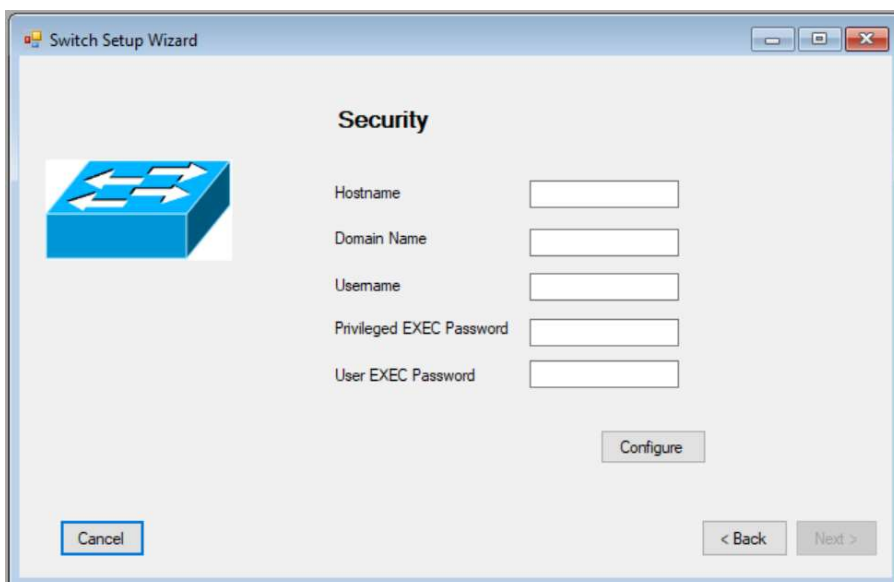
The screenshot shows the 'Switch Setup Wizard' window with the 'Network Configuration' tab selected. On the left is a blue switch icon. The main area contains the following fields:

- Default Gateway:
- VLAN section:
  - Name:
  - ID:
  - IP Address:
  - Mask:
  - Description:
- Access Interface Range:
  - From:
  - To:

At the bottom right is a 'Configure' button. At the bottom left is a 'Cancel' button. At the bottom center are '< Back' and 'Next >' buttons.

Figura 39. Ventana Configuración de Interfaz SVI.

En la interfaz de Seguridad, se especifica la información necesaria para establecer la configuración de SSH. Se indica el nombre de "Host", el dominio dentro del cual se encuentra el equipo, un nombre de usuario y las contraseñas correspondientes a los modos de configuración. Es posible observar en la figura 40.



The screenshot shows the 'Switch Setup Wizard' window with the 'Security' tab selected. On the left is a blue switch icon. The main area contains the following fields:

- Hostname:
- Domain Name:
- Username:
- Privileged EXEC Password:
- User EXEC Password:

At the bottom right is a 'Configure' button. At the bottom left is a 'Cancel' button. At the bottom center are '< Back' and 'Next >' buttons.

Figura 40. Ventana de Configuración de Seguridad.

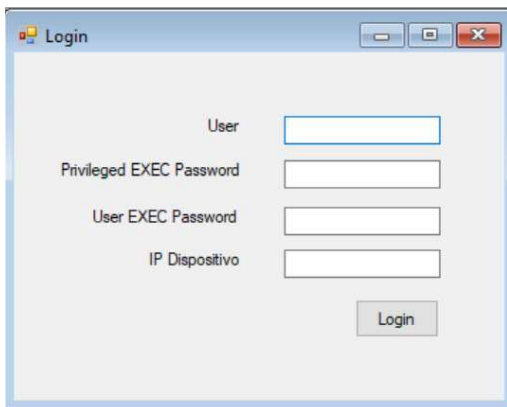
Con esta última ventana, se termina el procedimiento de integración y es posible iniciar la configuración del dispositivo a través del agente de configuración.

#### 4.4.2. Agente de configuración

El agente de configuración permite establecer los parámetros básicos de conmutación, que, a su vez, establecen las características propias de una red de núcleo, distribución y acceso.

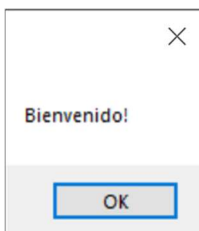
##### 4.4.2.1. Inicio de sesión

Al igual que en el caso del enrutador, es necesario validar autenticaciones para ingresar al equipo. Se verifica la información ingresada por el usuario y la información almacenada en el dispositivo al que se pretende conectar. Para ello se propone la siguiente disposición de controles. Se observa en la figura 41.



*Figura 41.* Pantalla de Inicio de Sesión

Una vez validado, aparece una pantalla que indica el éxito del ingreso, se observa la figura 42.



*Figura 42.* Pantalla de Acceso Permitido



Caso contrario, se da un mensaje de error, similar al que se puede observar en la Figura 43.



Figura 43. Pantalla de Acceso Denegado.

#### 4.4.2.2. Pantalla de configuración

Al igual que en el “router” la pantalla de configuración padre presenta una estructura de nodos, basada en la jerarquía de los comandos de los dispositivos con sistema operativo Cisco IOS. El control utilizado es un “TreeView”, el mismo que permite desplegar de manera ordenada las diferentes opciones de configuración del dispositivo, en función del nivel en que se encuentren. Las pantallas de las distintas configuraciones aparecen en el panel de la derecha, a medida que se seleccionan, se observa en detalle en la figura 44.



Figura 44. Pantalla de Configuración General.

##### 4.4.2.2.1. Configuración inicial

Las variables de configuración inicial incluyen, el nombre del dispositivo, el dominio en el cual se encuentra, si se desea búsqueda de DNS, el mínimo número de

caracteres para contraseñas y un mensaje de alerta en caso de acceso no autorizado. Es posible identificar en la figura 45.

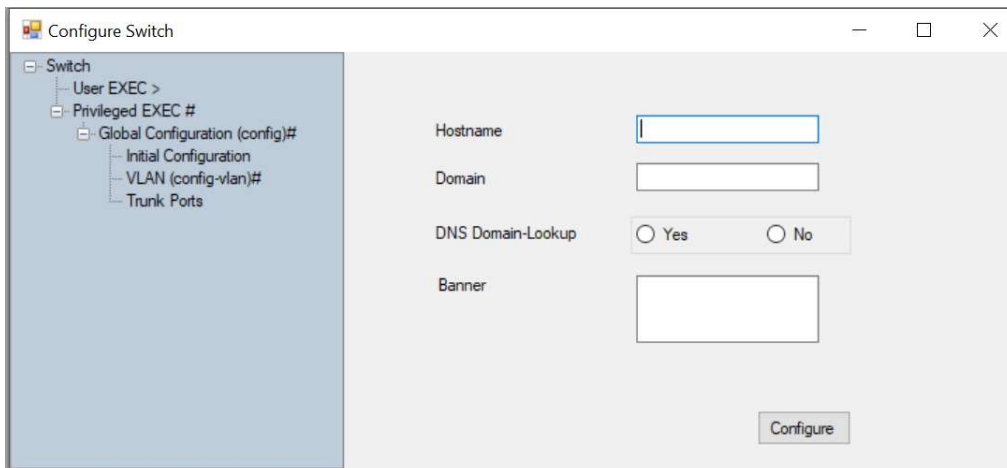
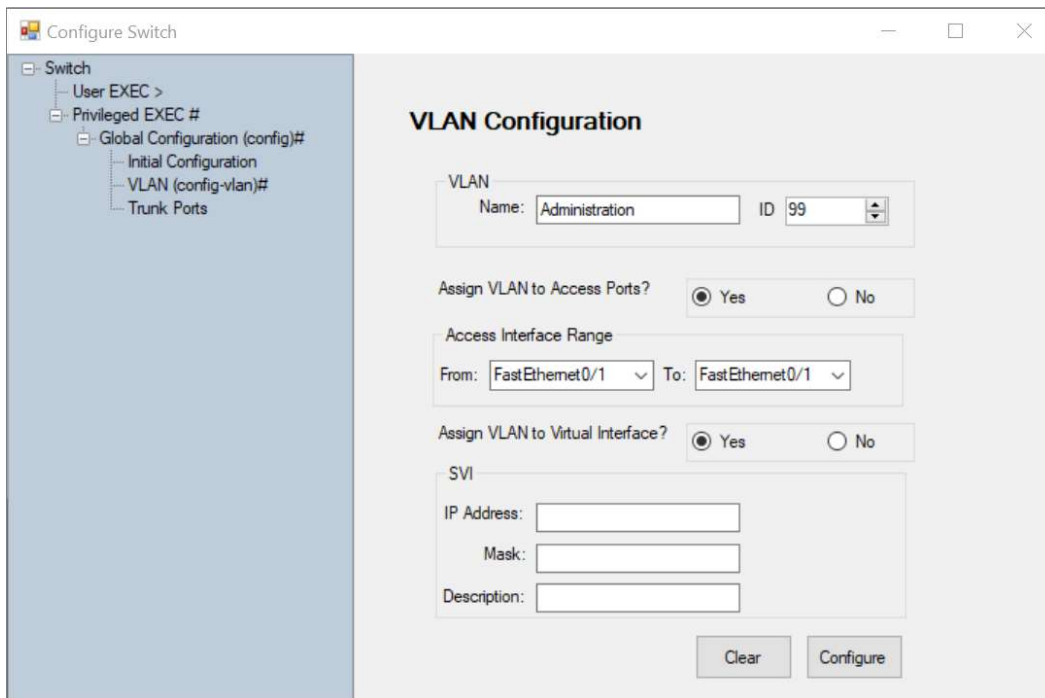


Figura 45. Pantalla de Configuración Inicial.

#### 4.4.2.2.2. Configuración de VLANs

El panel de configuración de “Virtual Local Area Network” permite la creación de nuevas VLAN y la adición de características a la misma. Existe un cuadro de texto, donde se detalla el nombre y un control de tipo “numericUpDown” que valida que el Id. de VLAN sea ingresado entre los valores de 1 y 4096. En ocasiones no es necesario agregar puertos de acceso a las VLANs, por ello existe la posibilidad de asignar o no interfaces físicas. Asimismo, existen ocasiones donde no es necesaria la asignación de una interfaz de red virtual (SVI). Por lo tanto, se da la opción de escoger si se le ingresa o no, configuraciones de IP a determinada Interfaz Virtual. Se observa a continuación en la figura 46.



*Figura 46.* Pantalla de Configuración VLAN

#### 4.4.2.2.3. Configuración de puertos troncales

Primeramente, se escoge la interfaz que se asigna como puerto troncal, utilizando el cuadro de combo. Luego, se indica la Id. VLAN nativa en el control numérico. Y como en ocasiones es necesario asignar varias virtual LAN, el menú de VLAN permitidas agrega distintas Id. con el botón más azul ([+]). Con el botón equis rojo ([X]), se puede borrar la última VLAN agregada en la lista. Es posible identificar en detalle en la figura 47, a continuación.

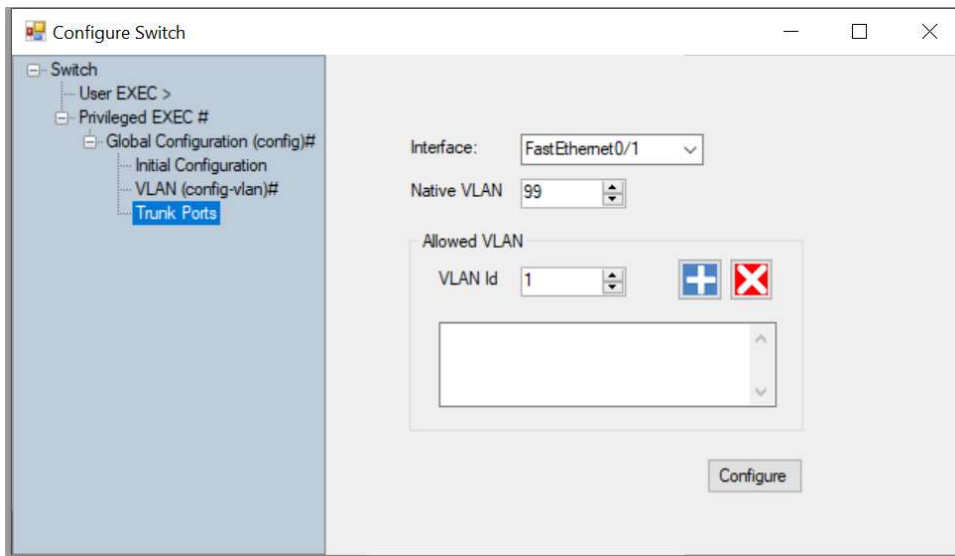


Figura 47. Pantalla de Configuración de Puertos Troncales.

#### 4.5. Agente de monitoreo

Es necesario observar las fluctuaciones en capacidades de los dispositivos de red, esto permite detectar algún tipo de anomalía que pudiese ocurrir durante las operaciones. Por ello se presenta una ventana que permite observar en tiempo real el rendimiento en CPU y RAM de los equipos de red, se identifica en la figura 48.

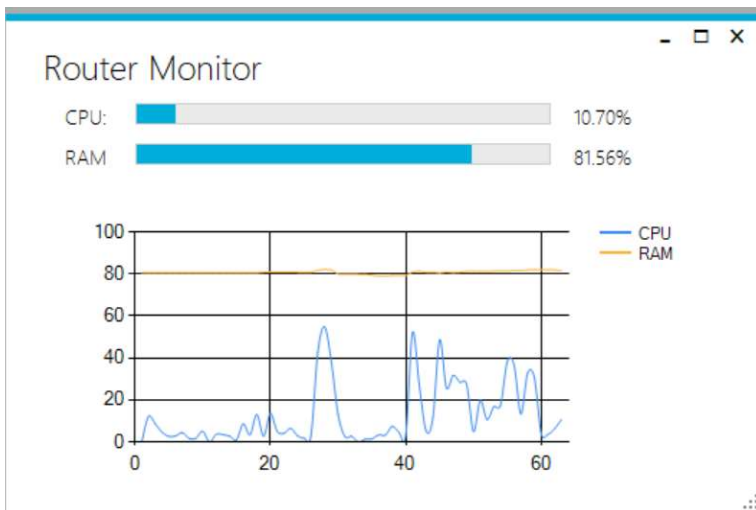


Figura 48. Pantalla de Monitoreo

## 4.6. Infraestructura

Con el propósito de facilitar el desarrollo del software, es necesario contar con una infraestructura, donde sea posible efectuar las pruebas, a medida que se vayan desarrollando los módulos. Para ello se contempla la posibilidad de virtualizar los dispositivos, debido a que el acceso a equipos físicos es limitado. Existe una plataforma propia de Cisco denominada OnePK all-in-one-vm la cual incluye máquinas virtuales de “Routers” Cisco en su interior.

Inicialmente se descarga el software de la página de Cisco: <https://developer.cisco.com/site/onepk> y se extrae:

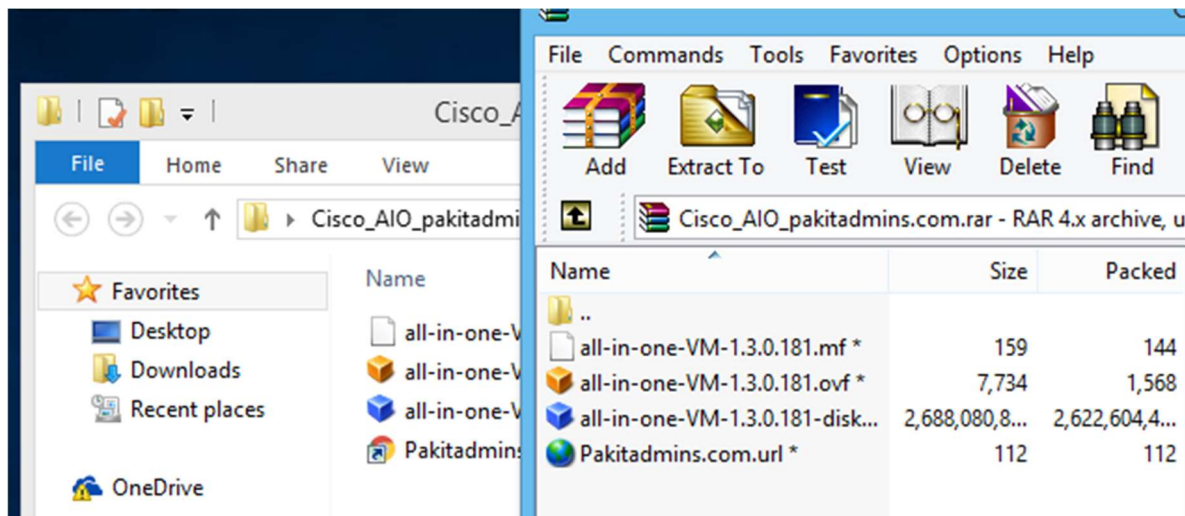


Figura 49. Extracción de Máquina Virtual.

Luego, se importa desde VirtualBox para poder revisar los contenidos de la máquina virtual. Desde el menú principal: File> Import Appliance y se selecciona el archivo descomprimido anteriormente. Obsérvese la figura 50.

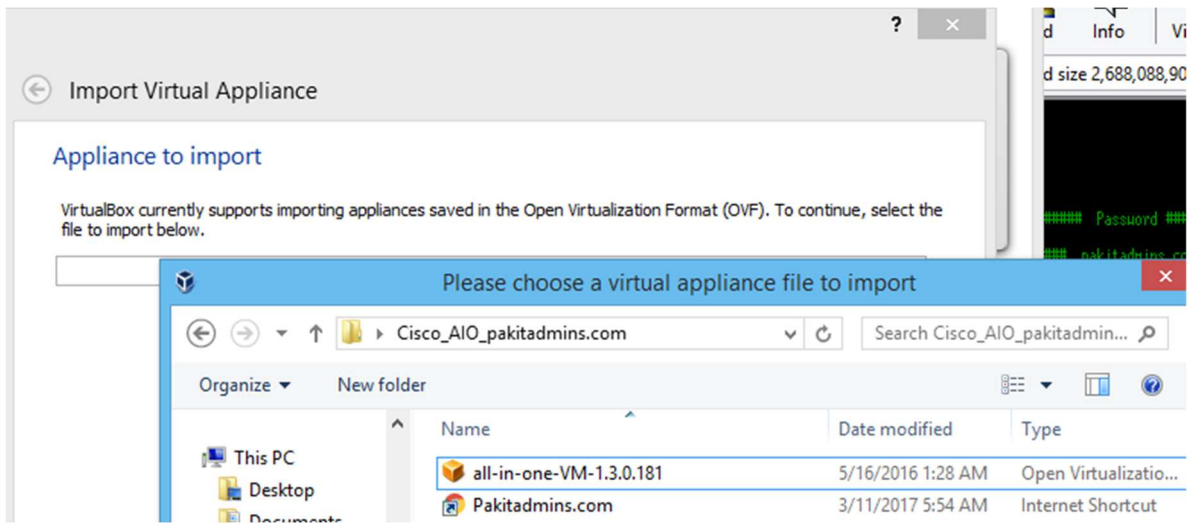


Figura 50. Importe de Máquina Virtual.

Una vez ha sido importada la máquina virtual, se inicia desde el panel de VirtualBox donde aparece la pantalla de inicio de sesión. La contraseña es: cisco123. Es posible identificar la figura 51.

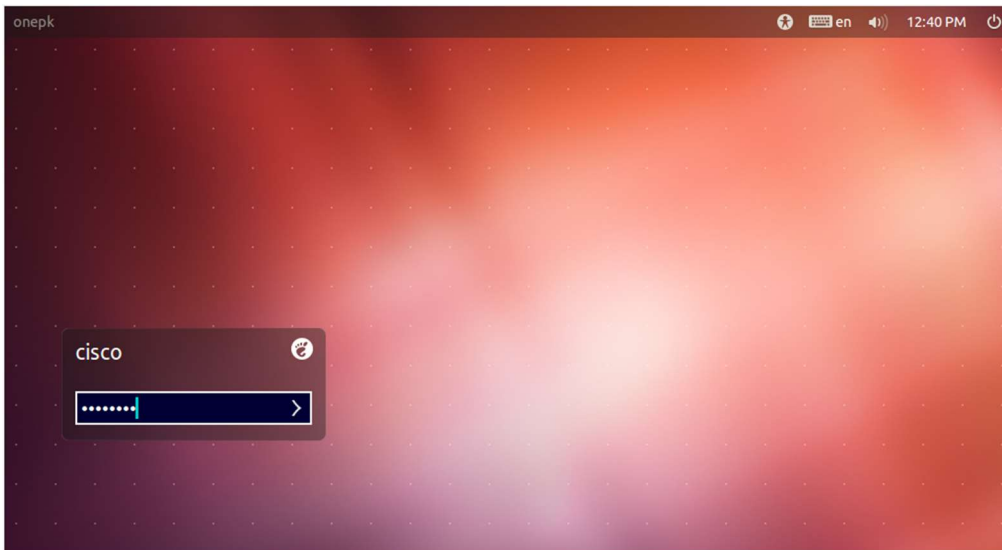
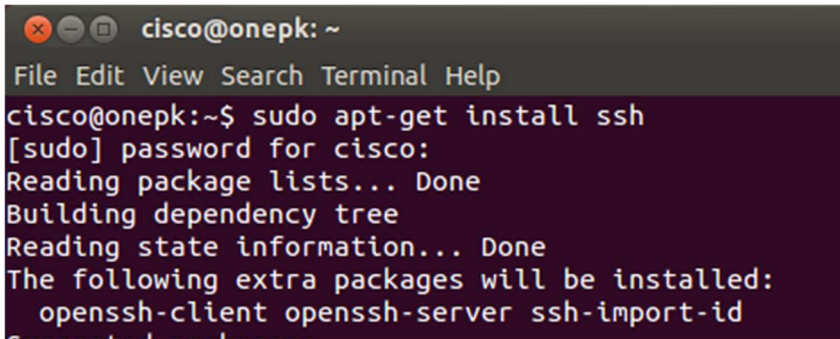


Figura 51. Inicio de Sesión en Máquina Virtual.

Dentro de la máquina virtual, es necesario instalar SSH con el propósito de extraer el sistema operativo de IOS. Se puede observar la figura 52 y se utiliza el comando:

```
$ sudo apt-get install ssh
```



```

cisco@onepk: ~
File Edit View Search Terminal Help
cisco@onepk:~$ sudo apt-get install ssh
[sudo] password for cisco:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  openssh-client openssh-server ssh-import-id

```

Figura 52. Ejecución de Comando Terminal.

Ahora ya es posible acceder a la máquina virtual desde WinSCP a través de SFTP, utilizando la dirección IP correspondiente y las credenciales:

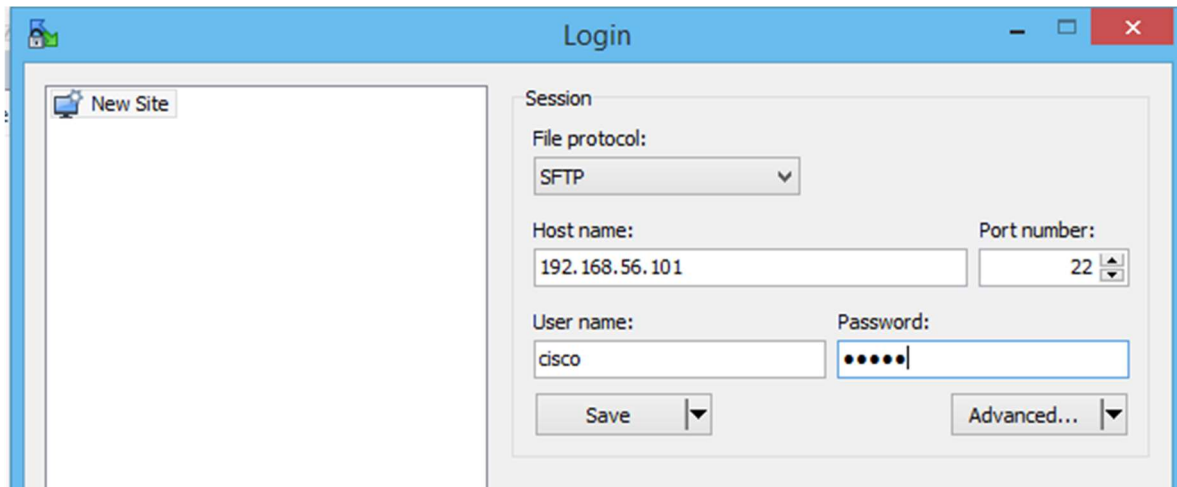


Figura 53. Acceso Desde WinSCP.

Cuando se accede al servidor desde el programa WinSCP, se encuentra la ubicación: `/usr/share/vmcloud/data/images/`. Se obtiene el archivo `vios-adventerprisek9-m` y se extrae. La documentación de Cisco indica que se debe importar en un servidor ESXi o KVM, pero se encuentra que es posible utilizarlo con VMware Workstation también. Por lo tanto, se importa desde el menú:

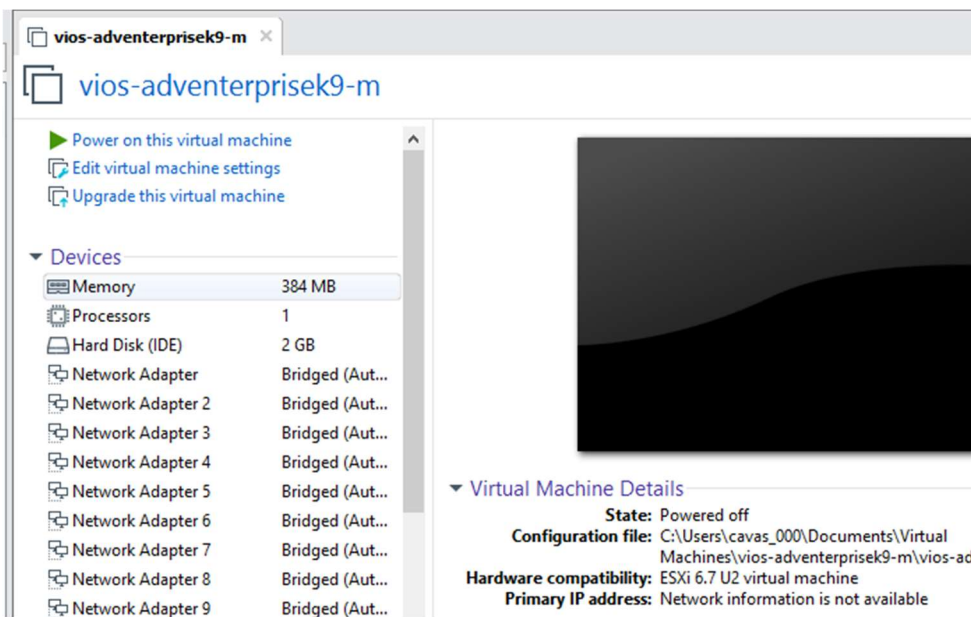


Figura 54. Panel de Administración de Máquinas Virtuales.

Adicionalmente, se le agrega una interfaz serial para poder ingresar al vIOS. Desde Virtual Machine Settings> Add...>Serial Port. Se configura un nombre de “pipe”:  
`\\.\pipe\com_1`

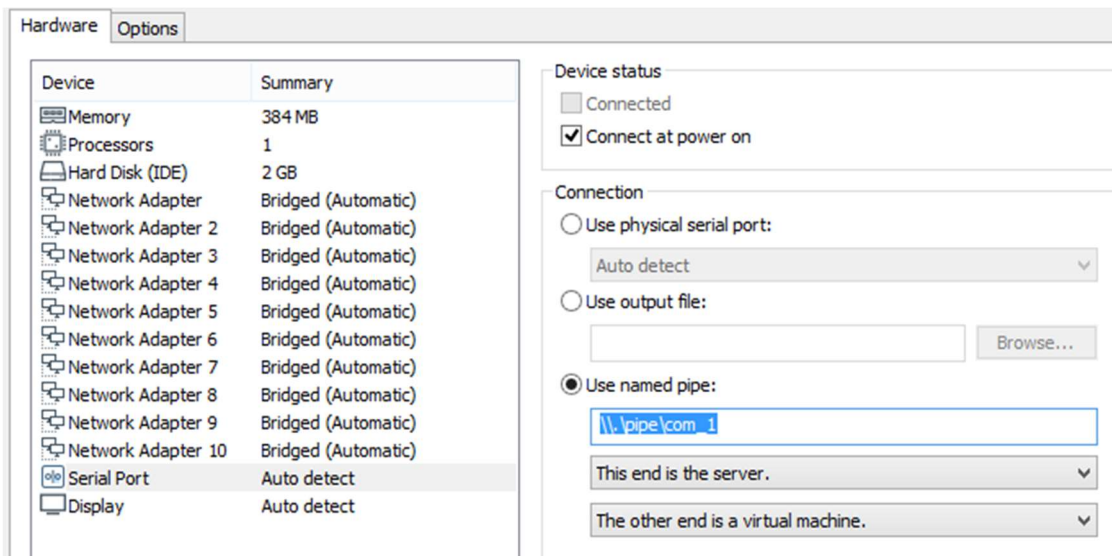
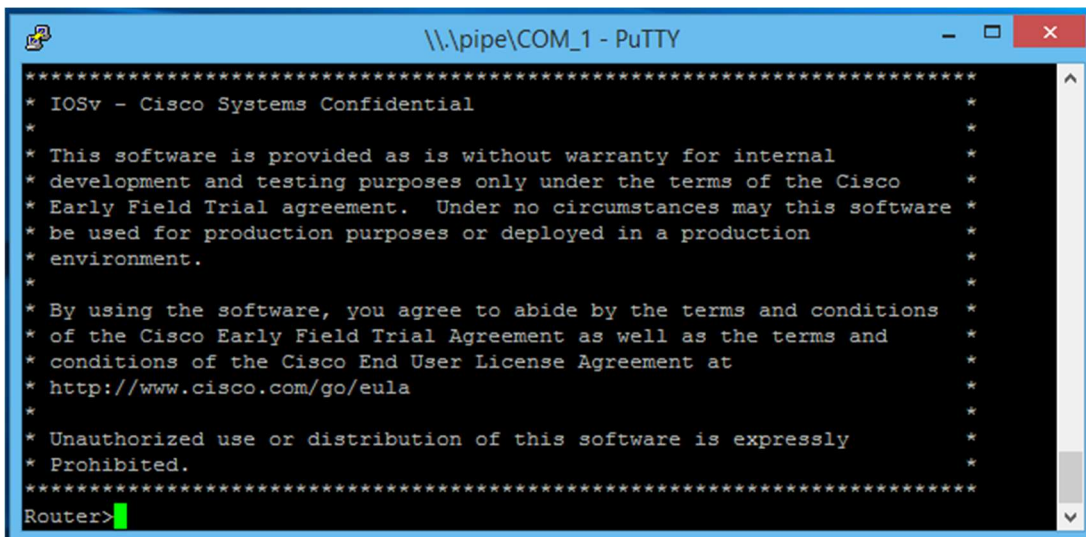


Figura 55. Creación de Puerto Serial.

Ya es posible acceder desde un programa que permita comunicación serial como “Putty”. Se observa que se tiene un dialogo típico de un Enrutador Cisco y es debido a que, efectivamente es el sistema operativo IOS, está trabajando de manera virtual.





```
\\.\pipe\COM_1 - PuTTY
*****
* IOSv - Cisco Systems Confidential
*
* This software is provided as is without warranty for internal
* development and testing purposes only under the terms of the Cisco
* Early Field Trial agreement. Under no circumstances may this software
* be used for production purposes or deployed in a production
* environment.
*
* By using the software, you agree to abide by the terms and conditions
* of the Cisco Early Field Trial Agreement as well as the terms and
* conditions of the Cisco End User License Agreement at
* http://www.cisco.com/go/eula
*
* Unauthorized use or distribution of this software is expressly
* Prohibited.
*****
Router>
```

Figura 56. CLI Putty.

El resultado, es el medio de desarrollo que se genera, se puede observar en el diagrama de implementación a continuación, en la figura 57.

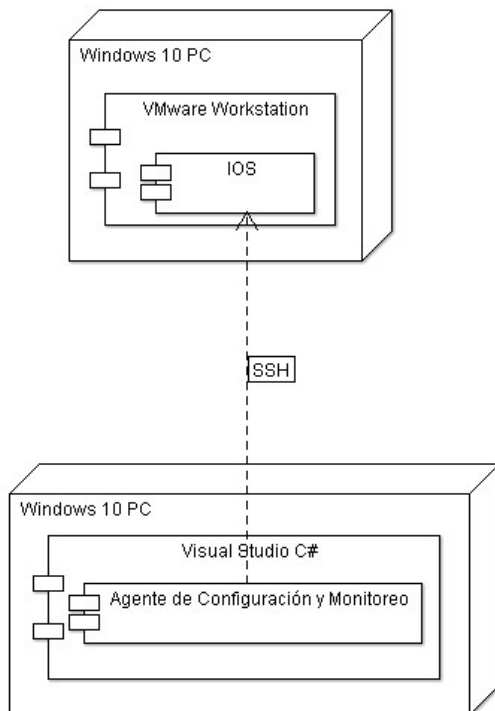
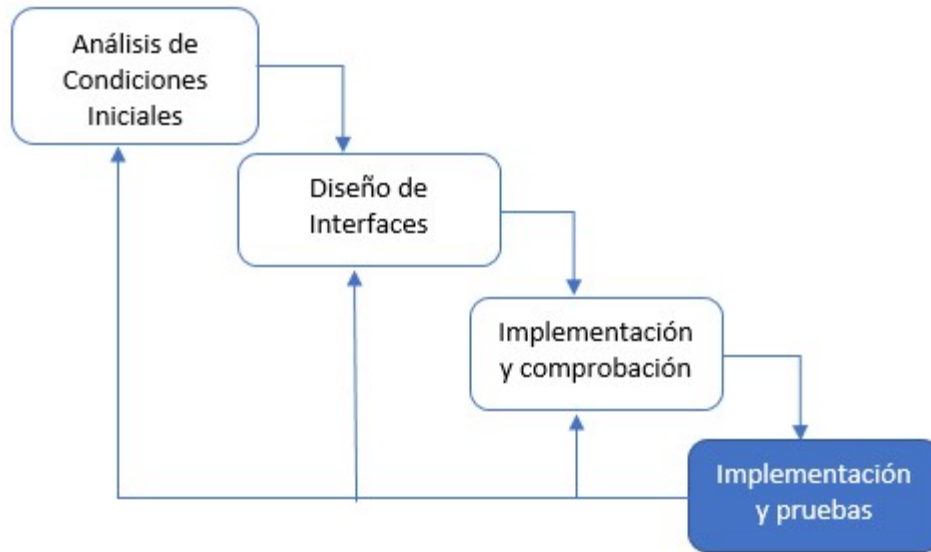


Figura 57. Diagrama de Implementación.

## 5. CAPITULO V: IMPLEMENTACIÓN Y PRUEBAS

Los procedimientos para la fase de Implementación y pruebas es posible observarlas en la figura 58. Más adelante se detalla el procedimiento efectuado.



*Figura 58.* Modelo Cascada

Para el proceso de implementación y pruebas, se plantean dos redes LAN, una en Quito y otra en Guayaquil. Las dos redes independientes, están unidas por un enrutador que supone el ISP. Las redes locales, tienen dos niveles de conmutación, una capa de distribución y una capa de acceso. Adicionalmente, se agregan distintas VLANs que representan departamentos organizacionales. Se observa en el diagrama topológico de la Figura 69.

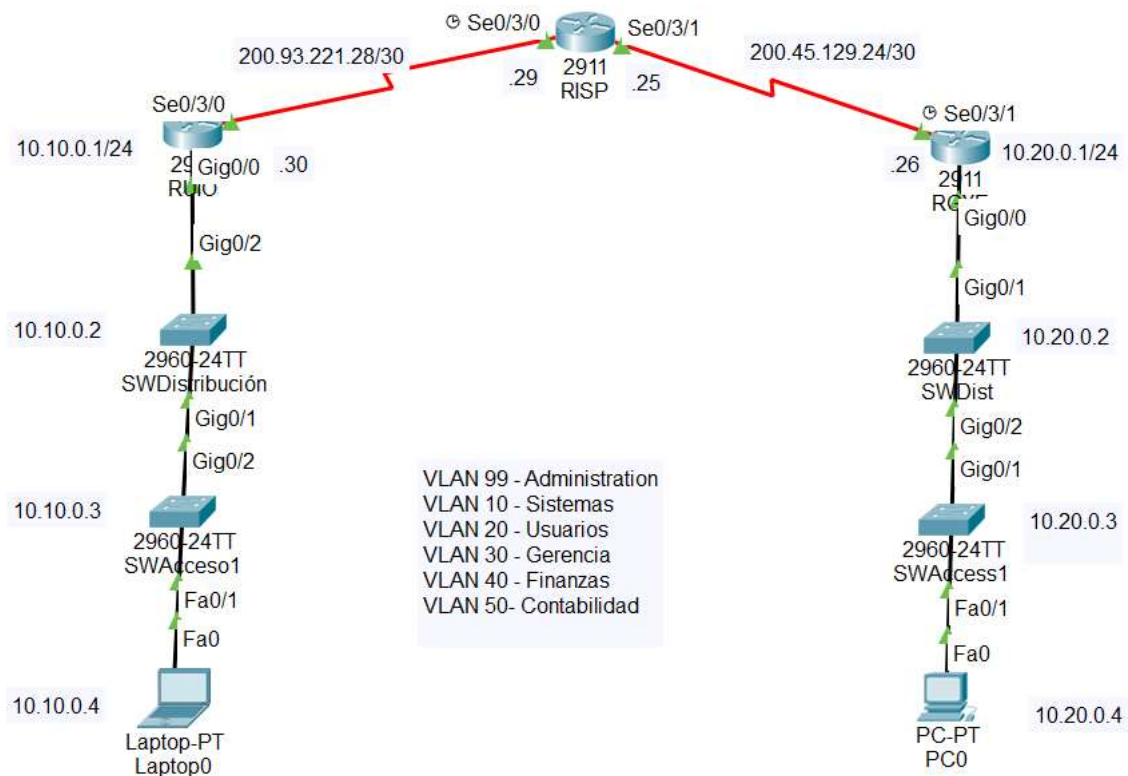


Figura 59. Diagrama Topológico Red Simulada.

La simulación se efectúa en el laboratorio con equipos Cisco Catalyst 2960, para los conmutadores y Cisco 2900, para los enrutadores. La disposición de los equipos físicos de acuerdo con la topología se puede observar en la figura 60 de topología física a continuación.



Figura 60. Topología Física.

Se preparan los equipos de la topología, retirando previamente las configuraciones. Es posible observar la terminal en la figura 61, con el uso de los comandos:

```
#write erase
```

```
#reload
```

```
Switch>ena
Switch#write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
*Mar 1 00:09:39.174: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]

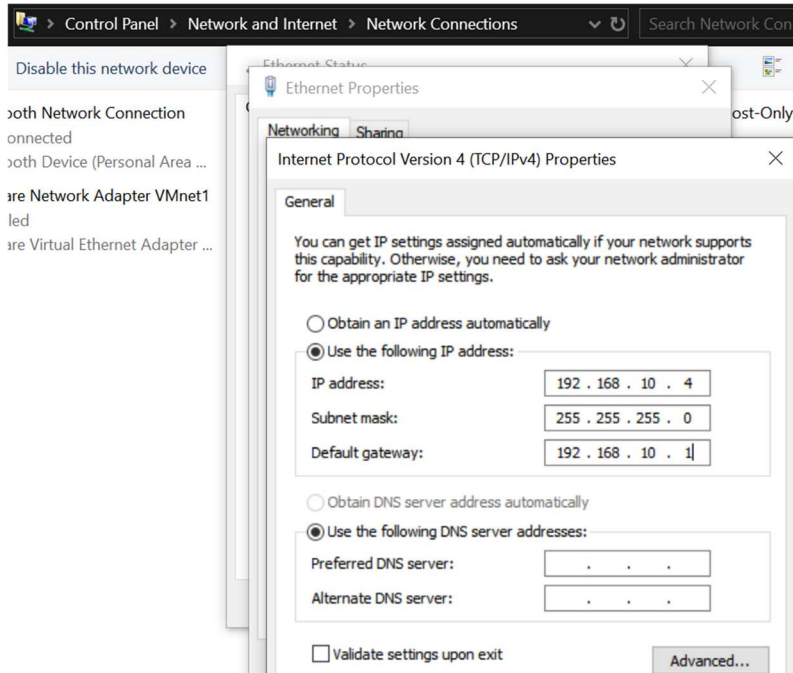
*Mar 1 00:10:19.817: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload command.
```

Figura 61. Ejecución de Comandos.

### 5.1. Incorporación de dispositivos

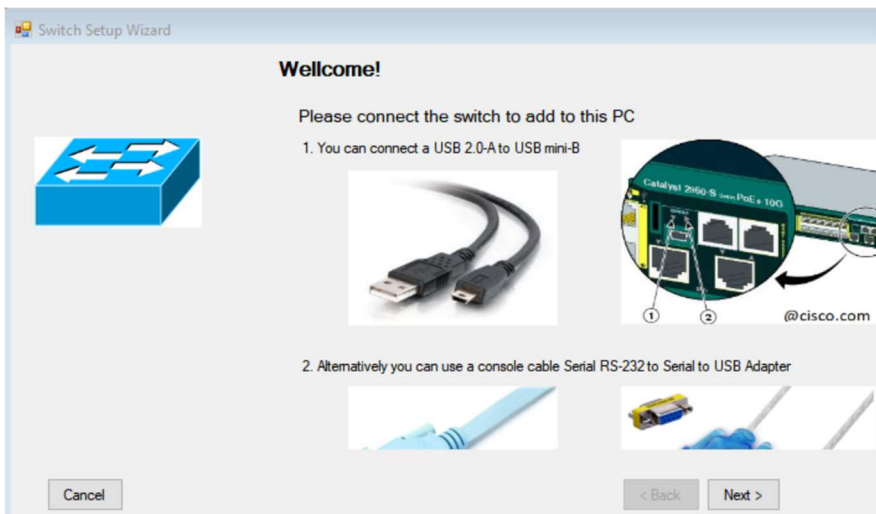
Se comienza por configurar el ordenador que contiene el programa de administración según la topología propuesta. Se accede en el menú de Windows: Panel de Control > Red e Internet > Conexiones de Red > Ethernet >

Propiedades>IPv4. Y se le asigna la dirección IP: 10.10.10.4/24 para la interfaz ethernet y Puerto de salida por defecto:10.10.10.1, como se observa a continuación en la figura 62.



*Figura 62.* Configuración de Red PC.

Una vez hecho esto, se accede al agente de adición para agregar el primer dispositivo que es el SWAcceso1. En la ventana de Dispositivos> Switch> Agregar Switch. Muestra la pantalla de bienvenida, donde indica que se debe conectar el dispositivo al ordenador de administración utilizando un puerto de consola y un cable serial. Se observa la figura 63.



*Figura 63.* Pantalla de Bienvenida

En la ventana de configuración de red se indica la información correspondiente. Se observa la figura 64.

*Figura 64.* Configuración de SVI.

Al dar clic en [Configure] aparece una ventana donde indica las configuraciones realizadas en el dispositivo. Se deja esta ventana activada en la etapa de pruebas, para verificar la configuración, pero se puede desactivar posteriormente. Se puede evidenciar en la figura 65.

```
Switch> ena
Switch#
Switch#
Switch#configure terminal
Enter configuration commands, one per line. End with (
Switch(config)#
Switch(config)#
Switch(config)#ip default-gateway 192.168.10.1
Switch(config)#
Switch(config)#
Switch(config)#vlan 99
Switch(config-vlan)#
Switch(config-vlan)#
Switch(config-vlan)#name Administration
Switch(config-vlan)#
Switch(config-vlan)#
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#
Switch(config)#interface vlan 99
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#ip address 192.168.10.3 255.255.255.0
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#no shutdown
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#description Switch de Acceso 1
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#
Switch(config)#
Switch(config)#interface range FastEthernet0/22-24
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#switchport mode access
Switch(config-if-range)
```

*Figura 65.* Verificación de la Ejecución.

También se despliega un pequeño diálogo indicando que se ha configurado correctamente. Se procede seleccionando el botón [Next>]. Aparece la pantalla de seguridad, en la figura 66, donde se ingresa la información correspondiente al SWAcceso1. Para el propósito de toda la práctica, se utiliza el usuario: usuario y la contraseña: clave.

Security	
Hostname	<input type="text" value="SWAccess1"/>
Domain Name	<input type="text" value="udla.ec"/>
Username	<input type="text" value="usuario"/>
Privileged EXEC Password	<input type="text" value="clave"/>
User EXEC Password	<input type="text" value="clave"/>
<input type="button" value="Configure"/>	

```

ena
Switch#
Switch#
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#
Switch(config)#hostname SWAccess1
SWAccess1(config)#
SWAccess1(config)#
SWAccess1(config)#ip domain-name udla.ec
SWAccess1(config)#
SWAccess1(config)#
SWAccess1(config)#crypto key generate rsa
The name for the keys will be: SWAccess1.udla.ec
Choose the size of the key modulus in the range of 360 to 4096
General Purpose Keys. Choosing a key modulus greater than 5
take
a few minutes.

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

```

*Figura 66.* Configuración de Parámetros de Seguridad y Validación.

Se encuentra que, en un conmutador de núcleo o distribución, no necesariamente es necesario asignar puertos de acceso a la interfaz de administración, por lo cual se debe dar la opción de establecer o no si la VLAN tiene puertos de acceso asignados.

Se procede con el siguiente dispositivo, que es el Router de borde de la sede Quito. Dispositivos> Router> Agregar Router. De igual manera, se observa una ventana de bienvenida, que indica que es necesario conectar el cable por puerto serial y se procede. La pantalla de bienvenida se identifica a continuación en la Figura 67.





Figura 67. Ventana de Bienvenida

En la ventana de Conexión, se indica el puerto serial y clic en [Conectar]. Aparece un dialogo indicando la validez de la conexión. Se procede con [Next>], así como se observa en la figura 68.

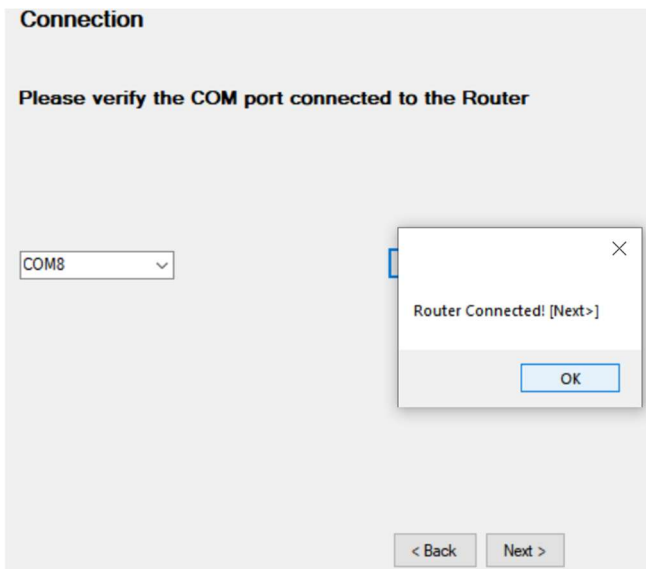


Figura 68. Ventana de Comunicación Serial.

Ahora, es necesario indicar los parámetros de red y la interfaz a utilizar para dichos parámetros. Se observa en la figura 69, a continuación.

### Network Configuration

Interface:

IP Address:

Mask:

Description:

```

ena
Router#
Router#
Router#configure terminal
Enter configuration commands, one per line. End with C/
Router(config)#
Router(config)#
Router(config)#Interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#
Router(config-if)#description Gateway LAN
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#exit
Router#
Router#
Router#exit

```

Figura 69. Configuraciones de Interfaz de Red y Validación.

Se ingresan los parámetros de identificación y autenticación en el menú de Seguridad. Es posible identificar los comandos ejecutados junto con la información ingresada en la forma identificada en la Figura 70.

### Security

Hostname:

Domain Name:

Username:

Privileged EXEC Password:

User EXEC Password:

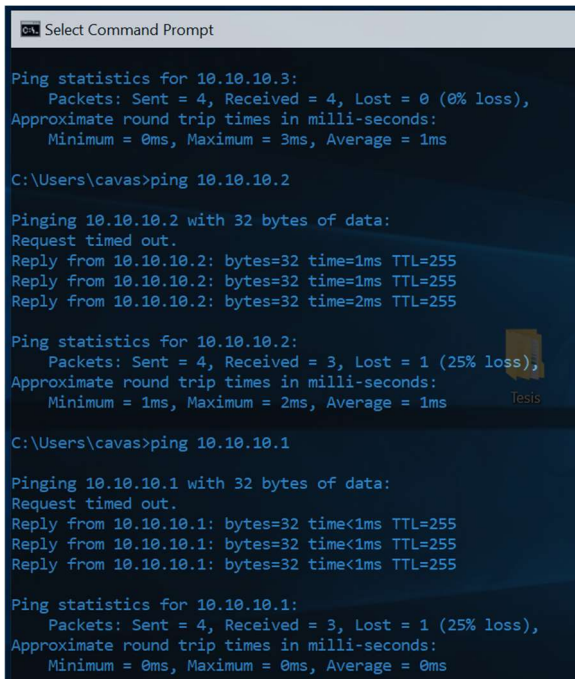
```

ena
Router#
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#hostname RUIO
RUIO(config)#
RUIO(config)#
RUIO(config)#ip domain-name udla.ec
RUIO(config)#
RUIO(config)#
RUIO(config)#crypto key generate rsa
The name for the keys will be: RUIO.udla.ec
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may
take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)
RUIO(config)#username usuario secret clave
RUIO(config)#
RUIO(config)#
RUIO(config)#line vty 0 15
RUIO(config-line)#
RUIO(config-line)#
RUIO(config-line)#transport input ssh
RUIO(config-line)#
RUIO(con

```

Figura 70. Configuraciones de Parámetros de Seguridad y Validación.

La manera en la que se agregan el resto de los dispositivos es la misma, únicamente varia la información individual de acuerdo con el diagrama topológico. Luego de agregar los dispositivos, se identifica que se tiene conectividad LAN. Se puede identificar en la figura 71.



```

Select Command Prompt

Ping statistics for 10.10.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\Users\cavas>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:
Request timed out.
Reply from 10.10.10.2: bytes=32 time=1ms TTL=255
Reply from 10.10.10.2: bytes=32 time=1ms TTL=255
Reply from 10.10.10.2: bytes=32 time=2ms TTL=255

Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\cavas>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:
Request timed out.
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
  
```

Figura 71. Conectividad LAN.

## 5.2. Configuración de dispositivos

Debido a que la configuración es similar en los distintos dispositivos y que básicamente lo único que varía es la información ingresada, se documenta la configuración de los dispositivos críticos de la topología.

### 5.2.1. Router de borde

Se inicia por configurar los enrutadores de borde de los respectivos sitios. Para ello, se accede a la ventana de: Dispositivos> Router> Configurar Router. Aparece una ventana de Inicio de Sesión donde se ingresa la información de autenticación y la IP del dispositivo. Según se puede observar en la figura 72.

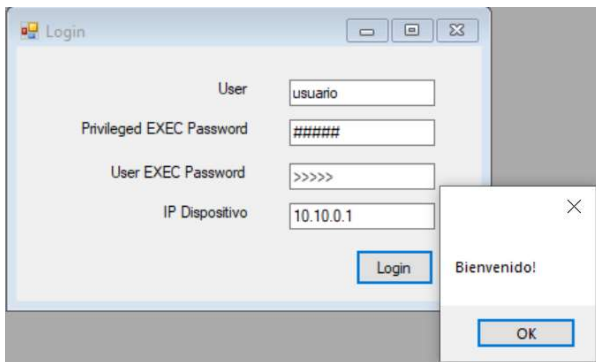


Figura 72. Inicio de Sesión.

Una vez ingresado, se configura la interfaz de conexión con el ISP, y se agrega la dirección IP correspondiente. Así como se puede observar a continuación en la figura 73.

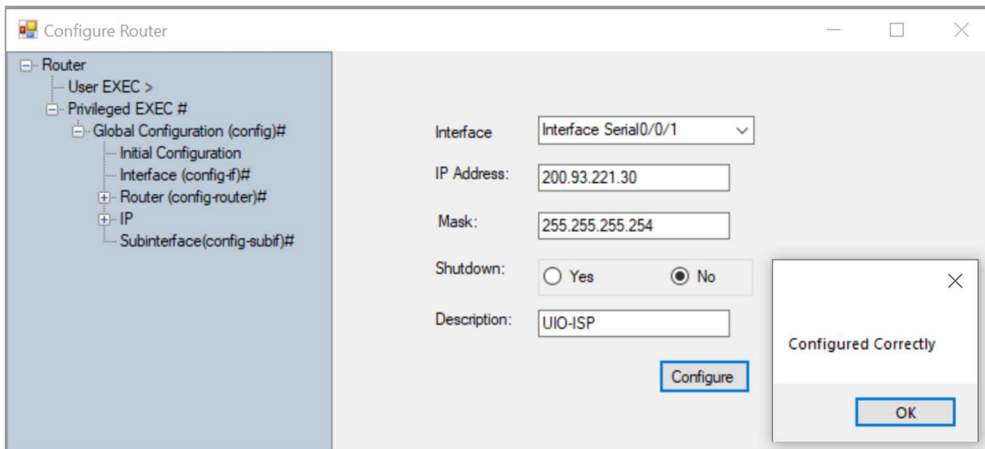


Figura 73. Configuración de Interfaces.

Se configura “Encapsulation 802.1Q” con las correspondientes direcciones de las VLAN, en el literal “Subinterface”. Y se agregan las subinterfaces correspondientes. Se observa la figura 74, donde se agrega la subinterfaz de Sistemas.

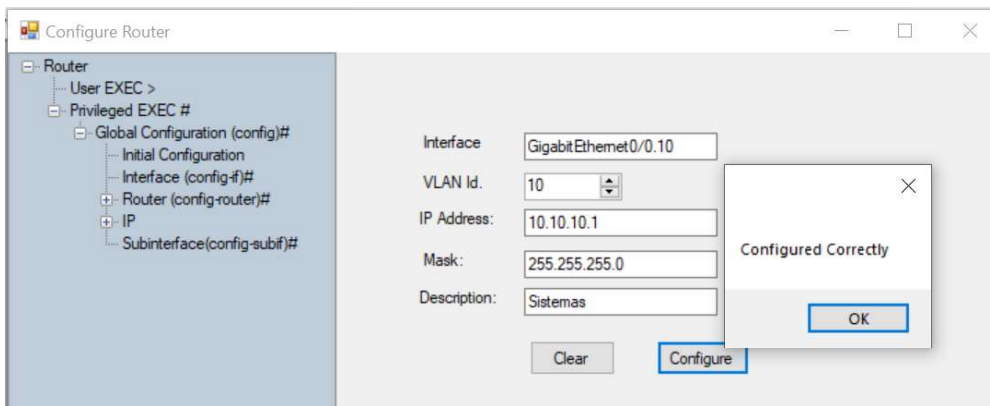


Figura 74. Configuración de Subinterfaces.

Luego se configura el servidor DHCP, el cual tiene diferentes grupos según las VLANs, Se reservan las primeras 10 direcciones. Es posible observar en la figura 75.

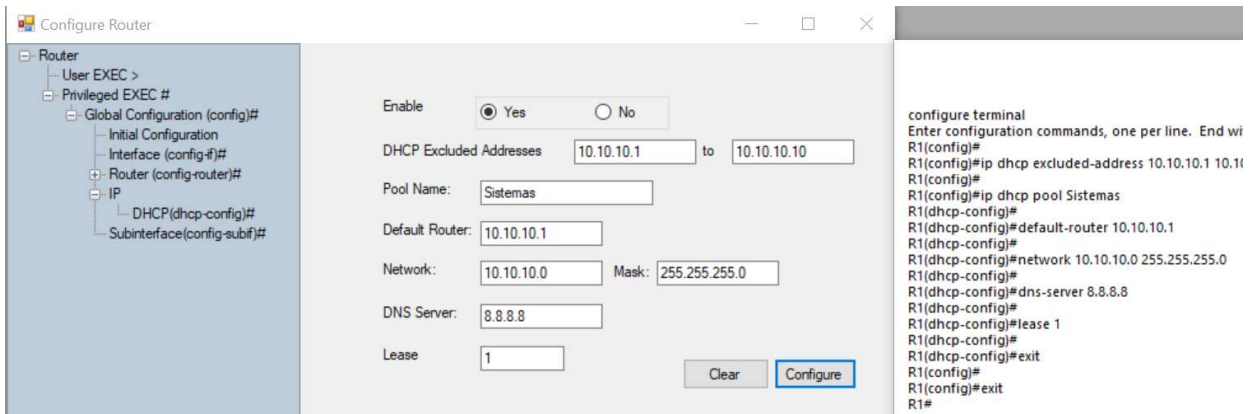


Figura 75. Configuración DHCP.

Con el propósito de obtener conectividad, se configura enrutamiento dinámico RIP. Se ingresan las redes directamente conectadas y la versión, como se observa a continuación en la figura 76.

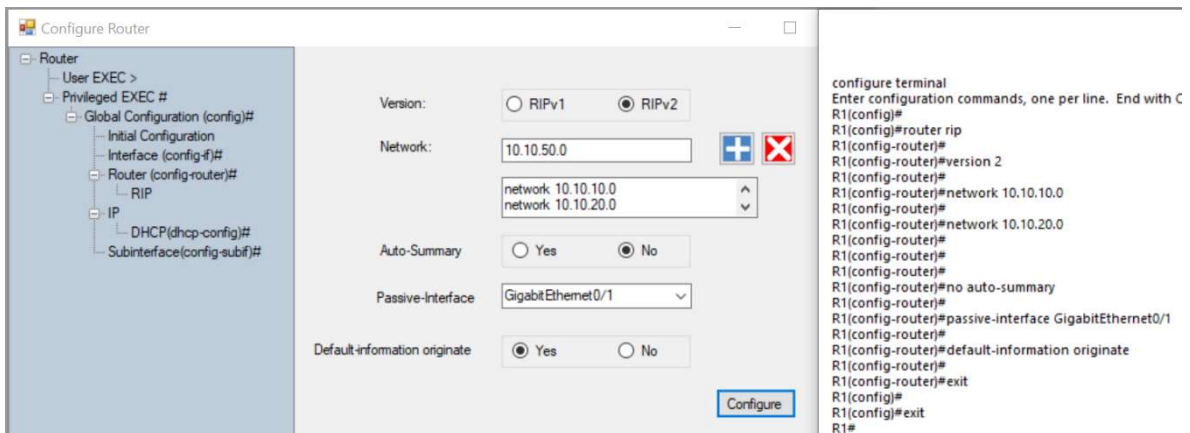


Figura 76. Configuración de Router RIP.

### 5.2.2. Switch de acceso 1

De igual manera, se ingresa la información de autenticación e identificación para acceder al panel de configuración. Desde el menú Dispositivos> Switch> Configurar. Aparece la ventana de “Log in” de la figura 77.

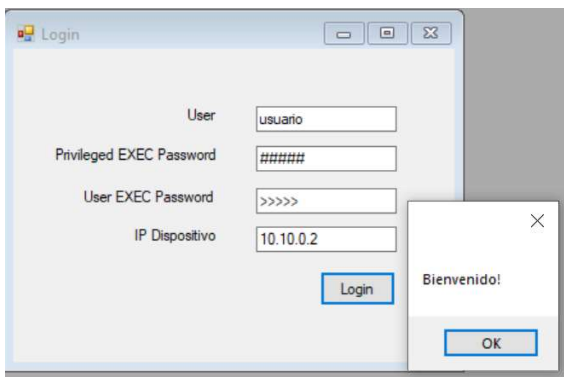


Figura 77. Inicio de Sesión.

En el menú de configuración de VLAN, se agregan las redes virtuales correspondientes. Además, se asigna puertos de acceso a las VLAN. Se observa la asignación de la VLAN 10 a continuación, en la figura 78.

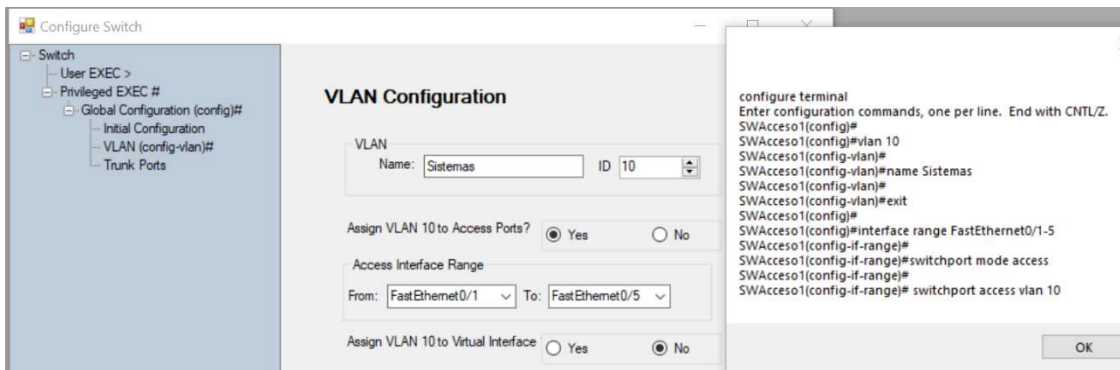


Figura 78. Configuración de VLAN.

Por último, se configura el enlace troncal del conmutador y se observa la validación de la ejecución de los comandos de la figura 79.

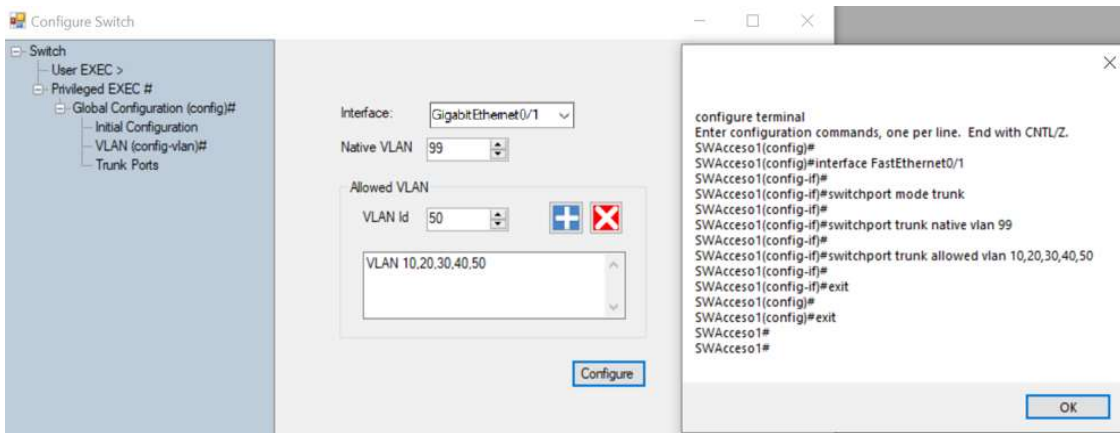


Figura 79. Configuración de Enlace Troncal.

## 6. CONCLUSIONES Y RECOMENDACIONES

### 6.1. CONCLUSIONES

Ha sido posible desarrollar un programa en Microsoft Visual Studio en lenguaje C#, que sirve como agente de configuración y monitoreo de dispositivos de red Cisco. Se logra efectuar con el acometido, a partir del cumplimiento de las diferentes fases propuestas. Análisis de las condiciones preexistentes, el diseño de las interfaces con su funcionalidad y la implementación en un medio físico para la probatura.

Inicialmente, se encuentra que existen modos de jerarquía dentro de los comandos Cisco, lo cual debe tenerse en cuenta al momento de programar las funciones. Esto es debido a que, si un comando se ejecuta en un modo de configuración que no le corresponde, el sistema operativo IOS, no lo reconoce. Asimismo, debido a que la sintaxis y algunos de los comandos, son los mismos para los dispositivos de conmutación y enrutamiento Cisco, los métodos que se utilizan para ambos son indistintos.

Además, ha sido posible establecer un medio de desarrollo a través de la obtención de la imagen de sistema operativo IOS y se virtualiza mediante el hipervisor tipo 2 VMware Workstation. En virtud de esto, resulta posible la implementación del sistema de configuración y monitoreo, en un medio simulado. Facilitando de esa manera, el testeo de los módulos de la solución.

El entorno de desarrollo integrado (IDE) de Microsoft Visual Studio, ha sido efectivo en brindar herramientas que son indispensables para la generación de las formas diseñadas en este trabajo. Las Formas de Windows, en conjunto con sus elementos programables, permiten brindar las funcionalidades requeridas. Específicamente, el componente de Árbol de Estructura de Datos permite organizar de manera



apropiada, los modos de estructura jerárquica de las configuraciones de sistema operativo Cisco IOS.

La utilización de Windows Visual Studio con lenguaje de desarrollo C#, otorga la clase SerialPort dentro de la librería System.IO. La cual permite establecer la comunicación serial entre el programa en cuestión con el dispositivo que se pretende configurar. Mas allá, aunque no exista una librería nativa de Microsoft Visual Studio para establecer sesiones SSH, a través de la utilización de “NuGets”, es posible implementar la librería Renci SSH.NET. La cual permite la cómoda utilización de métodos y clases necesarios para instaurar sesiones SSH entre el programa desarrollado y los dispositivos a configurar.

Mientras el dispositivo a configurar utilice comandos del sistema Cisco IOS, es posible utilizar la solución desarrollada. Esto excluye a los dispositivos Cisco que utilizan otros sistemas operativos, por ejemplo, CatOS o Cisco NX-OS. Propios de conmutadores antiguos y conmutadores Nexus, correspondientemente.

Luego de haber propuesto e implementado una red que abarca sectores LAN y WAN, además de configuraciones VLAN, con su debido enrutamiento. Es posible evidenciar que, las funcionalidades del sistema demuestran ser efectivas. Lo cual se consigue observar a través de los diálogos de ejecución de las configuraciones que han sido llevadas a cabo. Los archivos de configuración coinciden con los ajustes indicados en el programa de manera gráfica.

La optimización de la configuración y monitoreo permite obtener conectividad en una red organizacional, reduciendo el grado de error humano. Adicionalmente, se aumenta el grado de seguridad de la red, al inducir algunas configuraciones de seguridad de los dispositivos. Estas configuraciones podrían ser obviadas si se ajusta de manera manual. Asimismo, la seguridad a nivel de protocolo se brinda, al utilizar protocolos cifrados, tal como es SSH.

## 6.2. RECOMENDACIONES

Se ha desarrollado un entorno, compuesto de métodos, clases e interfaces tipo, las cuales podrían ser aprovechadas para extender las capacidades de alcance del propio software. Permitiéndole así a futuros encargados del proyecto, extender la cantidad de dispositivos admitidos y las configuraciones que se pueden efectuar.

Dado que la solución ha sido orientada hacia la funcionalidad, es decir, el “back-end” y más no el “front-end”. Existe la posibilidad de desarrollar la aplicación en un ambiente web, mejorando así la estética y la transparencia del sistema.

Se recomienda agregar un menú “drag and drop”, el cual permita visualizar los componentes de la red de manera gráfica. Esto le ayuda al usuario final a visualizar la red y poder identificar de manera más sencilla los equipos ingresados al sistema.

Debido a que se ha desarrollado la solución entorno a dispositivos de conmutación y enrutamiento Cisco, es posible agregar dispositivos de otras marcas, aumentando así el campo de acción del sistema.

Se recomienda extender el rango de configuraciones del agente, por motivo que se han incluido solamente los ajustes básicos de los equipos Cisco. En un nuevo proyecto se pudiese aumentar la cantidad de configuraciones que el sistema puede manejar.

## REFERENCIAS

- Abhishek, S. (2019). Software Defined Networking (SDN) Market 2019 Global Industry Size, Share, Trends, Sales Revenue, Competitive Landscape, Opportunity Assessment and Regional Forecast 2023. Recuperado el 30 de mayo 2019 de <https://www.marketwatch.com/press-release/software-defined-networking-sdn-market-2019-global-industry-size-share-trends-sales-revenue-competitive-landscape-opportunity-assessment-and-regional-forecast-2023-2019-03-14>.
- Andrew, T. (2009). Sistemas Operativos Modernos. Naucalpan de Juárez, Estado de México: Pearson Educación de México, S.A. de C.V.
- Axelson, J. (2007). Serial Port Complete. Madison, WI 53704: Lakeview Research LLC.
- Canavan, J. (2001). Fundamentals of Network Security. Boston • London: Artech House.
- Cisco. (2011). Cisco Configuration Professional Quick Start Guide. Recuperado el 2 de enero 2019, de Cisco Systems [https://www.cisco.com/c/en/us/td/docs/net\\_mgmt/cisco\\_configuration\\_professional/guides/CiscoCPqsg.html](https://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_configuration_professional/guides/CiscoCPqsg.html)
- Cisco. (2018). RIP Configuration Guide. Recuperado el 30 mayo 2019 de [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_rip/configuration/15-mt/irr-15-mt-book/irr-cfg-info-prot.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_rip/configuration/15-mt/irr-15-mt-book/irr-cfg-info-prot.html)
- Cisco. (2017). Cisco 2900 Series Integrated Services Routers Data Sheet. Recuperado el 30 de mayo 2019 de

[https://www.cisco.com/c/en/us/products/collateral/routers/2900-series-integrated-services-routers-isr/data\\_sheet\\_c78\\_553896.html](https://www.cisco.com/c/en/us/products/collateral/routers/2900-series-integrated-services-routers-isr/data_sheet_c78_553896.html)

Cisco. (2017). Cisco IOS Technologies. Recuperado el 4 de junio 2019 de <https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-technologies/index.html>

Cisco. (2018). What Is IT Security?. Recuperado el 31 de mayo de 2019 de <https://www.cisco.com/c/en/us/products/security/what-is-it-security.html>

Cisco. (2018). RIP Configuration Guide. Recuperado el 30 mayo 2019 de [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_rip/configuration/15-mt/irr-15-mt-book/irr-cfg-info-prot.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_rip/configuration/15-mt/irr-15-mt-book/irr-cfg-info-prot.html)

Cisco. (2018). Cisco Catalyst 2960-X Series Switches. Recuperado el 6 de junio 2019 de <https://www.cisco.com/c/en/us/products/switches/catalyst-2960-x-series-switches/index.html>

Deitel H., Deitel P. (2007). *Cómo Programar C#*. Naucalpan de Juárez, Edo. de México: Pearson Educación.

Ceballos, J. (2013). *Enciclopedia de Microsoft® Visual C#*. Madrid: RA-MA.

Goralski, W. (2009), *The Illustrated Network*, San Francisco- USA: Elsevier.

Göransson, P., Black, C. (2014). *Software Defined Networks A Comprehensive Approach*. Waltham USA: Elsevier.

Haroon, S. (Feb. 2014). Client-Server Model. IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, 67-71. Recuperado el 31 de mayo 2019, De semanticscholar Base de datos.

Laan, S. (2017). IT Infrastructure Architecture – Infrastructure Building Blocks and Concepts: Lulu Press Inc.

Levy, S. (2017). Graphical user interface. Recuperado el 6 de junio 2019 de <https://www.britannica.com/technology/graphical-user-interface>

Melonfire. (2006). Understanding the pros and cons of the Waterfall Model of software development. Recuperado el 6 de junio 2019 de <https://www.techrepublic.com/article/understanding-the-pros-and-cons-of-the-waterfall-model-of-software-development/>

Microsoft. (2019). SerialPort Class. Recuperado el 29 de mayo 2019 de <https://docs.microsoft.com/en-us/dotnet/api/system.io.ports.serialport?view=netframework-4.8>

Microsoft. (2019). Visual Studio 2019. Recuperado el 30 de mayo de 2019 de <https://visualstudio.microsoft.com/vs/>

Microsoft. (2019). Windows Forms. Recuperado el 4 de junio 2019 de <https://docs.microsoft.com/en-us/dotnet/framework/winforms/>

Microsoft. (2017). Windows Forms Controls. Recuperado el 30 de junio 2019 de <https://docs.microsoft.com/en-us/dotnet/framework/winforms/controls/>

Microsoft. (2018). Classes (C# Programming Guide). Recuperado el 4 de junio 2019 de <https://docs.microsoft.com/en-us/dotnet/csharp/programming-guide/classes-and-structs/classes>

Netacad. (2016). Introducción a las redes. Recuperado el 30 de mayo de 2019 de <https://static-course-assets.s3.amazonaws.com/ITN503/es/index.html#2.1.1.1>

Portnoy Matthew. (2017). Virtualization Essentials. Estados Unidos: Sybex.

R. D. Groves, (2015), Brief History of Computer Architecture Evolution and Future Trends, IBM, 5-9.

Refsnes Data. (2019). What is Command Line Interface (CLI)?. Recuperado el 30 de mayo de 2019 de [https://www.w3schools.com/whatis/whatis\\_cli.asp](https://www.w3schools.com/whatis/whatis_cli.asp)

Renci. (2016). SSH.NET. Recuperado el 4 de Julio 2019, de MIT: <https://github.com/sshnet/SSH.NET/>

Rouse, M. (2015). CIA triad. Recuperado el 4 de junio 2019, de <https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA>

Rumbaugh, J. (2007). Object-Oriented Modeling and Design. New York: Prentice-Hall.

Silberschatz, A. (2006). Fundamentos de Sistemas Operativos. España: McGraw-Hill.

Sommerville, I. (2011). Software Engineering. Boston Massachusetts: Pearson.

Strangio, C. (2012). The RS232 Standard A Tutorial with Signal Names And Definitions, CAMI Research Inc. Acton Massachusetts. Recuperado el 7 de junio 2019 de [http://www.camiresearch.com/Data\\_Com\\_Basics/RS232\\_standard.html#anchor1154232](http://www.camiresearch.com/Data_Com_Basics/RS232_standard.html#anchor1154232)

Techopedia. (2019). IT Infrastructure. Recuperado el 7 de junio 2019 de <https://www.techopedia.com/definition/29199/it-infrastructure>

VMware Inc. (2019). Virtualization. Recuperado el 7 de junio 2019 de <https://www.vmware.com/solutions/virtualization.html>

Wendell, O. (2017). CCNA Routing and Switching ICND2 200-105 Official Cert Guide. Indianápolis, USA: Pearson Education.

## **ANEXOS**



## CLASE CONEXION SERIAL

```
1. using System;
2. using System.Collections.Generic;
3. using System.IO.Ports;
4. using System.Linq;
5. using System.Text;
6. using System.Threading.Tasks;
7.
8. namespace CapaConexion
9. {
10.     public static class clsSerialConn
11.     {
12.         public static SerialPort puertocereale = new SerialPort();
13.
14.         public static bool openconn(string portname)
15.         {
16.             puertocereale.PortName = portname;
17.             puertocereale.Open();
18.             if (puertocereale.IsOpen)
19.             {
20.                 return true;
21.             }
22.             else
23.             {
24.                 return false;
25.             }
26.         }
27.
28.         public static void getready()
29.         {
30.             puertocereale.WriteLine(Environment.NewLine);
31.             System.Threading.Thread.Sleep(200);
32.             String strData = puertocereale.ReadExisting();
33.
34.             if (strData.Contains("initial configuration dialog?"))
35.                 write("no");
36.             if (strData.Contains("terminate autoinstall?"))
37.                 write("yes");
38.
39.             if (strData.Contains("RETURN"))
40.                 write("");
41.             if (strData.Contains("#"))
42.                 write("exit");
43.             if (strData.Contains("(config)#"))
44.             {
45.                 write("exit");
46.                 write("exit");
47.             }
48.             if (strData.Contains("(config-if)#"))
49.             {
50.                 write("exit");
51.                 write("exit");
52.                 write("exit");
53.             }
54.         }
55.     }
56.
```

```
57.     public static string writereurn(string command)
58.     {
59.
60.         puertocereal.WriteLine(Environment.NewLine);
61.         System.Threading.Thread.Sleep(200);
62.         String strData = puertocereal.ReadExisting();
63.
64.         if (strData.Contains("initial configuration dialog?"))
65.             puertocereal.WriteLine("no"+Environment.NewLine);
66.         return strData;
67.     }
68.
69.     public static void crypto()
70.     {
71.         puertocereal.WriteLine("crypto key generate rsa\n1024");
72.         //puertocereal.WriteLine("1024" + Environment.NewLine);
73.         System.Threading.Thread.Sleep(200);
74.
75.
76.     }
77.
78.     public static string read()
79.     {
80.         String strData = puertocereal.ReadExisting();
81.         return strData;
82.     }
83.
84.     public static bool isready()
85.     {
86.         puertocereal.WriteLine(Environment.NewLine);
87.         System.Threading.Thread.Sleep(200);
88.         String strData = read();
89.         if (strData.Contains(">"))
90.             return true;
91.         else
92.             return false;
93.     }
94.
95.     public static void write(string command)
96.     {
97.         if (puertocereal.IsOpen)
98.         {
99.             puertocereal.WriteLine(command + Environment.NewLine);
100.            System.Threading.Thread.Sleep(200);
101.        }
102.    }
103.
104.    public static void close()
105.    {
106.        puertocereal.Close();
107.    }
108.
109.    public static bool isopen()
110.    {
111.        if (puertocereal.IsOpen)
112.            return true;
113.        else
114.            return false;
115.    }
```

```

116.     }
117. }

```

## CLASE CONEXIÓN SSH

```

1. using System;
2. using System.Collections.Generic;
3. using System.Linq;
4. using System.Text;
5. using System.Threading.Tasks;
6. using Renci.SshNet;
7.
8. namespace CapaNegocio
9. {
10.     public static class clsSSHSession
11.     {
12.         private static SshClient sshClient = null;
13.         private static ShellStream shellStreamSSH = null;
14.         public static void createStream(string user, string password, string ipaddr
15. )
16.         {
17.             sshClient = new SshClient(ipaddr, int.Parse("22"), user, password);
18.             sshClient.ConnectionInfo.Timeout = TimeSpan.FromSeconds(120);
19.             sshClient.Connect();
20.             shellStreamSSH = sshClient.CreateShellStream("vt100", 80, 60, 800, 600
21. , 65536);
22.         }
23.         public static void write(string command)
24.         {
25.             shellStreamSSH.Write(command + "\r\n");
26.             shellStreamSSH.Flush();
27.             System.Threading.Thread.Sleep(100);
28.         }
29.     }
30.
31.     public static void flush()
32.     {
33.         shellStreamSSH.Flush();
34.     }
35.
36.     public static string read()
37.     {
38.         string read=shellStreamSSH.Read();
39.         return read;
40.     }
41.
42.     public static void closeSession()
43.     {
44.         shellStreamSSH.Close();
45.         sshClient.Disconnect();
46.     }
47. }

```

| 48. }

