

# **UNIVERSIDAD TÉCNICA DE COTOPAXI**

**CARRERA DE CIENCIAS DE LA INGENIERIA Y APLICADAS**

**TESIS DE GRADO PREVIO A LA OBTENCIÓN DEL TITULO DE  
INGENIERO EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES**

## **TÍTULO:**

**“CONFIGURACION DE UN ROUTER PARA OPTIMIZAR LA  
ADMINISTRACIÓN DE LA RED DE DATOS DEL CENTRO  
EXPERIMENTAL Y PRODUCCIÓN SALACHE (CEYPSA) DE LA  
UNIVERSIDAD TÉCNICA DE COTOPAXI”**

## **POSTULANTES:**

**Castellano Moreno Paúl César  
Vaca Armendáriz José Washington**

## **DIRECTOR:**

**ING. VERÓNICA TAPIA**

**ECUADOR - LATACUNGA**

**2008**

## AUTORIA

Los autores certifican que la investigación, redacción y propuesta del presente trabajo son de su exclusiva autoría.



---

Castellano Moreno

Paúl César

**CI:050198742-4**



---

Vaca Armendáriz

José Washington

**CI: 050175133-3**

## CERTIFICACIÓN

HONORABLE CONSEJO ACADÉMICO DE LA UNIVERSIDAD TÉCNICA  
DE COTOPAXI.

De mi consideración:

Cumpliendo con lo estipulado en el Capítulo IV, (Art. 9 literal f), del reglamento del curso profesional de la Universidad Técnica de Cotopaxi, informo que los postulantes, Castellano Moreno Paúl César y Vaca Armendáriz José Washington han desarrollado su Tesis de Grado de acuerdo al planteamiento formulado en el plan de tesis con el tema: "CONFIGURACION DE UN ROUTER PARA OPTIMIZAR LA ADMINISTRACIÓN DE LA RED DE DATOS DEL CENTRO EXPERIMENTAL Y PRODUCCIÓN SALACHE (CEYPSA) DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI", cumpliendo sus objetivos respectivos.

En virtud de lo antes expuesto considero que la presente tesis se encuentra habilitada para presentarse al acto de la defensa de tesis.



Ing. Verónica Tapia.

**DIRECTOR DE TESIS.**

Latacunga, abril del 2008

## AGRADECIMIENTO

A Dios, principio y fin de todo lo que conocemos.

Nuestro incondicional agradecimiento a la Universidad Técnica de Cotopaxi y las personas que de una u otra forma colaboraron pacientemente en desarrollo de este Trabajo, ustedes nos enseñaron o inspiraron todos los conceptos plasmados en este proyecto.

Gracias a todos nuestros docentes por su generosidad al entregarnos íntegros el tesoro de sus conocimientos, hoy que estamos fuera de nuestras aulas continuaremos trabajando “POR LA VINCULACIÓN DE LA UNIVERSIDAD CON EL PUEBLO.”

*Paúl C. Castellano M.*

*José W. Vaca A.*

## DEDICATORIA

Con amor incondicional dedico este trabajo a las mejores personas que he tenido el gusto de conocer....

A mi esposa Albi, a mis hijas Sayana y Samantha, ustedes me enseñan constancia para lograr los ideales y metas que me proponga... La verdad es que entre sus juegos y sonrisas se desarrolló la mayor parte de este proyecto.

A papá Gonzhita(+), mamá Laurita y a mis hermanos quienes son y serán fuente de inspiración en todos y cada uno de mis objetivos...

***Paúl Castellano Moreno***

A mi Señor, Jesús, quien me dio la fe, la fortaleza, la salud y la esperanza para terminar este trabajo.

A mi esposa, Mónica Fonseca, quien me brindó su amor, su cariño, su estímulo y su apoyo constante. Su cariño, comprensión y paciente espera para que pudiera terminar este proyecto son evidencia de su gran amor.

A mi hijo(a) que esta por nacer y representa lo más importante, valioso y especial que tenemos con mi esposa en nuestra vida.

A mis padres, Pastora y Hugo quienes me enseñaron desde pequeño a luchar para alcanzar mis metas. Mi triunfo es el de ustedes.

***José Vaca Armendáriz***

# INDICE

Págs.

## CAPITULO I

### TRANSMISIÓN DE DATOS

1.1	Generalidades de transmisión de datos.....	1
1.1.1	Tipos de Transmisión.....	2
1.1.1.1	La transmisión analógica .....	2
1.1.1.2	La transmisión digital .....	2
1.1.2	Medios de Transmisión Guiados .....	3
1.1.2.1	Par trenzado .....	3
1.1.2.2	Pares trenzados apantallados y sin apantallar .....	3
1.1.2.3	Cable coaxial .....	4
1.1.2.4	Fibra óptica .....	4
1.2.	Redes informáticas .....	5
1.2.1	Software de aplicaciones .....	6
1.2.2	Software de red .....	7
1.2.3	Hardware de red .....	7
1.3	Topología de las redes .....	8
1.3.1	Topología de Bus .....	9
1.3.2	Topología de Anillo .....	10
1.3.3	Topología en Estrella .....	11
1.4	Tipos de redes .....	11
1.4.1	LAN (Local Área Network): Redes de Área Local .....	12
1.4.2	MAN (Metropolitan Área Network): Redes de Área Metropolitana ..	13
1.4.3	WAN (Wide Area Network): Redes de Amplia Cobertura .....	13
1.5.	Modelos de Comunicación .....	13
1.5.1	Modelo OSI .....	14
1.6	Protocolos de comunicación .....	15
1.6.1	Características .....	16
1.6.2	Funciones .....	16
1.6.3	Tipos de Protocolos .....	19
1.6.4	Protocolo TCP/IP .....	19

1.7	Router .....	20
1.7.1	Funciones de un ruteador .....	21
1.7.2	Beneficios del Ruteador .....	22
1.7.3	Tipos de Router .....	22
1.7.4	Características de los dos tipos de Router .....	23
1.7.5	Segmentado de Subredes con Routers .....	24
1.8.	Seguridad informática .....	24
1.8.1	Mecanismos de Seguridad .....	26
1.8.1.1	Prevención .....	26
1.8.1.2	Detección .....	26
1.8.1.3	Recuperación .....	27
1.8.2	Servidor de Seguridades .....	27
1.8.2.1	Características del servidor de seguridad .....	28
1.8.2.2	Clases de servidor de seguridad .....	28

## **CAPITULO II**

### **METODOLOGÍA DE LA INVESTIGACIÓN**

2.1.	Introducción .....	30
2.2.	Población a Investigar .....	32
2.3.	Operacionalización de las variables .....	33
2.3.1	Variable Independiente .....	33
2.3.2	Variable Dependiente .....	34
2.4	Recolección y procesamiento de Datos .....	35
2.4.1	Presentación y análisis de resultados .....	36
2.5	Conclusiones .....	44
2.6	Recomendaciones .....	45
2.7.	Introducción a los requerimientos .....	45
2.7.1	Requerimientos .....	46
2.7.2	Objetivo .....	47
2.7.3	Usuarios .....	47
2.7.4	Metas .....	48
2.7.5	Funciones del Software .....	48

2.7.6	Elementos del software .....	49
2.7.7	Funciones básicas del Router .....	49
2.7.8	Elementos del Router .....	50
2.8	Introducción a los Casos de Uso .....	51
2.8.1	Casos de uso .....	51
2.8.2	Actividades y dependencias .....	51
2.8.3	Actores .....	52
2.8.4	Diagrama de los casos de uso .....	52
2.8.5	Descripción de procesos .....	53
2.8.6	Casos de uso de alto nivel .....	53
2.8.7	Casos de uso expandidos .....	53
2.9	Inicio de un ciclo de desarrollo .....	54
2.10	Modelo conceptual de la Aplicación .....	55
2.10.1	Agregación de las asociaciones .....	57
2.10.2	Agregación de los atributos .....	58
2.11.	Diccionario de datos .....	59
2.12	Diagramas de secuencia del sistema .....	60
2.13	Análisis e interpretación operativa de resultados .....	61
2.14	Verificación de la Hipótesis .....	63

### **CAPITULO III**

#### **LA PROPUESTA**

3.1	Modelo de Análisis y Diseño .....	65
3.2	Algunos aspectos del diseño del sistema. ....	66
3.3	Mapeo de los diseños para codificación .....	67
3.4.	Implementación y pruebas .....	68
3.4.1	Introducción .....	68
3.4.2	Contenido .....	69
3.4.3	Usuarios del Router CISCO 2811 .....	69
3.4.4	Uso del módulo .....	70
3.4.5	Visión general del documento .....	70
3.5	Generalidades de los Router CISCO .....	71

3.5.1	Introducción .....	71
3.5.2	Principios de un Router .....	72
3.5.2.1	La familia Sistemas Operativos (IOS) .....	72
3.5.2.2	Numeración T .....	72
3.5.2.3	Numeración S .....	73
3.5.2.4	Numeración XR .....	73
3.5.3	Partes de un Router .....	73
3.5.4	Actualizaciones de un Router .....	74
3.6	Router CISCO 2811 .....	74
3.6.1	Especificaciones de un Router CISCO Serie 2811 .....	75
3.6.2	Conectividad del Router Cisco 2811 del CEYPSA .....	76
3.6.3	Instalación del SDM de CISCO .....	77
3.6.3.1	Requerimientos para instalación de SDM de CISCO .....	78
3.6.4	Instalación de SDM de CISCO .....	79
3.6.5	Instalación de JAVA .....	84
3.7	Modos de Acceso al Router .....	87
3.7.1	Modo Línea de Comando - EXEC .....	87
3.7.1.1	Acceso al IOS .....	87
3.7.1.2	Comandos CISCO del Modo de Usuario .....	90
3.7.1.3	Comandos CISCO Modo EXEC Privilegiado .....	92
3.7.1.4	Comandos CISCO Modo de Configuración Global .....	95
3.7.1.5	Comandos CISCO Submodo de Configuración de Interfaz .....	97
3.7.1.6	Comandos CISCO Submodo de Configuración de Línea .....	99
3.7.1.7	Comandos CISCO de Edición y otros .....	99
3.7.2	Modo Grafico – SDM .....	100
3.7.2.1	Acceso SDM .....	100
3.8	Información del Router CEYPSA .....	104
3.8.1	Pantalla de Información General .....	104
3.8.2	Información Estadística del Router .....	106
3.8.2.1	Opciones de Configuración .....	106
3.8.3	Configuración de las Interfaces del Router CEYPSA.....	107
3.8.4	Configuración del Firewall del Router CEYPSA .....	108

3.8.5	Enrutamiento del Router CEYPSA .....	109
3.8.6	Configuración del NAT en el Router CEYPSA .....	110
3.8.7	Configuración de las Tareas Adicionales del Router CEYPSA .....	112
3.9	Configuraciones del Router CISCO 2811 del Centro de Experimentación y Producción Salache .....	114
3.9.1	Diseño de la Red de Datos del CEYPSA .....	114
3.10	Transformación de los Diagramas en Código. ....	117
3.11	Conclusiones .....	134
3.12	Recomendaciones .....	135
3.13	Bibliografía .....	136
3.13.1	Bibliografía citada .....	136
3.13.2	Bibliografía consultada .....	136
3.13.3	Bibliografía virtual .....	137

## ANEXOS

Anexo 1 Certificación del Administrador de Red del CEYPSA

Anexo 2 Acta de entrega – recepción del Router

Anexo 3 Certificación de traducción

Anexo 4 Guía de Usuario del Router 2811

## INDICE DE FIGURAS

Grafico 1.1 Topología de Bus.....	10
Grafico 1.2 Topología de Anillo.....	10
Grafico 1.3 Topología en Estrella.....	11
Grafico 1.4 Modelo OSI.....	15
Grafico 1.5 Protocolo TCP/IP.....	20
Grafico 1.6 Segmentación.....	24
Grafico 2.1 Problemas de la red de datos.....	36
Grafico 2.2 Información segura.....	37
Grafico 2.3 Dispositivo de seguridad.....	38
Grafico 2.4 Agilización de la información.....	39
Grafico 2.5 Destino de información.....	40
Grafico 2.6 Red disponible.....	41
Grafico 2.7 Importancia de un router.....	42
Grafico 2.8 Implementación de un router.....	43
Grafico 2.9 Representación y análisis de resultados.....	44
Grafico 2.10 Diagrama de Casos de Uso del negocio.....	52
Grafico 2.11 Modelo conceptual inicial del proyecto.....	56
Grafico 2.12 Asociación administrador administración.....	57
Grafico 2.13 Asociación administrador router.....	57
Grafico 2.14 Modelo conceptual aplicado al sistema.....	58
Grafico 2.15 Conceptos y Atributos.....	59
Grafico 2.16 Diagrama de secuencia para el caso de uso: Administración..	61
Grafico 3.1 Casos de uso Administración.....	66
Grafico 3.2 Vista clásica de una arquitectura de tres capas.....	67
Grafico 3.3 Diagrama de Despliegue.....	68
Grafico 3.4 Router Cisco 2811.....	74
Grafico 3.5 Conectividad parte frontal.....	76
Grafico 3.6 Conectividad parte posterior.....	77
Grafico 3.7 Instalación de SDM de Cisco.....	79
Grafico 3.8 Pantalla de bienvenida.....	80

Grafico 3.9 Licencia de Software.....	80
Grafico 3.10 Tipo de instalación.....	81
Grafico 3.11 Ubicación destino SDM.....	82
Grafico 3.12 Inicio instalación SDM.....	82
Grafico 3.13 Fin instalación SDM Cisco.....	83
Grafico 3.14 Ingreso software SDM Cisco.....	84
Grafico 3.15 Acondicionamiento para la instalación de JAVA.....	85
Grafico 3.16 Aceptación de la licencia de JAVA.....	85
Grafico 3.17 Proceso de instalación de JAVA.....	86
Grafico 3.18 Fin del proceso de instalación JAVA.....	86
Grafico 3.19 Definición nombre conexión / hyperterminal.....	87
Grafico 3.20 Definición puerto a utilizar / hyperterminal.....	88
Grafico 3.21 Definición de parámetros COM1 / hyperterminal.....	88
Grafico 3.22 Acceso al router / hyperterminal.....	89
Grafico 3.23 Ingreso al SDM Cisco.....	101
Grafico 3.24 Ingreso de la IP para proceso de carga SDM.....	101
Grafico 3.25 Ingreso al web browser del router.....	102
Grafico 3.26 Proceso de acceso a la información del router 1.....	103
Grafico 3.27 Proceso de acceso a la información del router 2.....	103
Grafico 3.28 Información general del router CEYPSA.....	104
Grafico 3.29 Opción de configuración del router CEYPSA.....	106
Grafico 3.30 Configuración de las interfaces router CEYPSA.....	107
Grafico 3.31 Configuración del Firewall router CEYPSA.....	108
Grafico 3.32 Enrutamiento router CEYPSA.....	109
Grafico 3.33 Configuración del NAT en el router CEYPSA.....	111
Grafico 3.34 Tareas adicionales router CEYPSA 1.....	112
Grafico 3.35 Tareas adicionales router CEYPSA 2.....	113
Grafico 3.36 Tareas adicionales router CEYPSA 1.....	113
Grafico 3.37 Diseño de la red de datos del CEYPSA.....	114

## ÍNDICE DE TABLAS

Tabla No 1.1 Tipos de router.....	23
Tabla No 2.1 Población.....	32
Tabla No 2.2 Variable independiente.....	33
Tabla No 2.3 Variable dependiente.....	34
Tabla No 2.4 Problema de la red de datos.....	36
Tabla No 2.5 Información segura.....	37
Tabla No 2.6 Dispositivo de seguridad.....	38
Tabla No 2.7 Agilización de la información.....	39
Tabla No 2.8 Destino de información.....	40
Tabla No 2.9 Red disponible.....	41
Tabla No 2.10 Importancia de un router.....	42
Tabla No 2.11 Implementación de un router.....	43
Tabla No 2.12 Funciones básicas del router.....	48
Tabla No 2.13 Atributos del sistema.....	49
Tabla No 2.14 Funciones básicas del router.....	50
Tabla No 2.15 Elementos del router.....	50
Tabla No 2.16 Curso normal de los eventos de la Administración.....	54
Tabla No 2.17 Ciclo de desarrollo del proyecto.....	55
Tabla No 2.18 Glosario de Términos.....	60
Tabla No 3.1 Características del router Cisco 2811.....	75
Tabla No 3.2 Comandos CISCO modo usuario.....	90
Tabla No 3.3 Comandos CISCO modo privilegiado.....	92
Tabla No 3.4 Comandos CISCO modo configuración global.....	95
Tabla No 3.5 Comandos CISCO submodo de configuración interfaz.....	97
Tabla No 3.6 Comandos CISCO submodo de configuración en línea.....	99
Tabla No 3.7 Comandos CISCO de edición y otros.....	99

## RESUMEN

Este documento es una Especificación de Requisitos Software (ERS) para el Router CISCO 2811 del CEYPSA-UTC, el mismo que se constituye en el medio oficial para proveer documentación técnica a los usuarios del Router CISCO 2811 de la Red de Datos del CEYPSA, resalta sus características más significativas y describe las instrucciones de diseño.

En el Capítulo I empezamos con un estudio bibliográfico de todos los aspectos que tienen que ver con la Transmisión de Datos, la misma que trata del traslado de información de un lugar a otro mediante diferentes dispositivos de comunicación para las Redes Informáticas, se incluye en este capítulo el estudio de Tipos y Medios de Transmisión Guiados, en donde se permite que varios usuarios puedan acceder a recursos y dispositivos determinados en los distintos tipos de redes que según los autores las han clasificado de acuerdo a la cobertura geográfica en LAN, MAN, WAN, y de los principales Modelos y Protocolos de Comunicación, de ahí que la aplicación de la nuestro tema de investigación se fundamenta principalmente en el Modelo OSI y el Protocolo TCP/IP.

Basados en lo expuesto anteriormente encaminamos el estudio y aplicación del proyecto hacia los Routers, sus funciones, beneficios y tipos, como puntos de partida hacia la Seguridad informática.

El Capítulo II contiene toda la Metodología de la Investigación, cimentada en los indicadores arrojados por la aplicación de las Variables Dependientes e Independientes se dio paso a los conceptos para la aplicación de las distintas Técnicas de Investigación (experimentación, observación de campo), así como para la recolección de datos (encuestas entrevistas), posteriormente se llegó a las principales conclusiones y recomendaciones de acuerdo con los requerimientos necesarios para cumplir con el objetivo de nuestro trabajo de investigación

A fin de incrementar la viabilidad de obtener una utilidad adecuada, el desarrollo de la Tesis se basa en un conveniente modelado del análisis y diseño, ello significa que durante la Configuración del Router tienen cabida los prototipos de Rational Rose para el modelado del diseño UML, las modernas herramientas de simulación interactiva para Routers Cisco que ofrecen un excelente ambiente para examinar rápidamente métodos alternos, y normalmente vale la pena dedicar tiempo al diseño para la codificación.

En el Capítulo III se encuentra la Propuesta de la Tesis de Grado en donde se incluye toda la documentación operativa para el uso de Router CISCO 2811 del CEYPSA a ser adoptada por los usuarios del mismo, basados principalmente en el uso y aplicación de herramientas operativas necesarias para la aplicación como la instalación del SDM que permite la configuración en modo gráfico del equipo (Router and Security Device Manager SDM) y el acondicionamiento para la instalación de Java de Java Sun Microsystem

Finalmente tenemos el manual de usuario del Router Cisco 2811 del CEYPSA el mismo que cumple dilatadamente con los requerimientos de los administradores y usuarios de la Red de Datos. En cuanto a la conformidad y cobertura de las necesidades del Router, satisface de forma clara las expectativas del Administrador con los siguientes parámetros:

- Ostentan un método estándar para la seguridad de la información
- Poseen control para administrar el Router
- Mantienen un mecanismo de comunicación entre los procesos y el software
- Gozan de visualización grafica del control del Router.

## ABSTRACT

This document is a Specification of Requirements Software (ERS) for the Router CISCO2811 of the CEYPSA-UTC, the same one that is constituted in the official means to provide technical documentation to the users of the Router CISCO2811 of the Net of Data of the CEYPSA, stands out its more significant characteristics and it describes the design instructions.

In the Chapter I begins with a bibliographical study of all the aspects that the have to do with the Transmission of Data, the same one that is about the transfer of information from a place to another by means of different communication devices for the Computer Nets, it is included in this chapter the study of Types and Guided Means of Transmission where it is allowed several users to consent to resources and devices determined in the different types of nets that have classified them according to the geographical covering according to the authors in LAN, MAN, WAN, and of the main Models and Protocols of Communication, with the result that the application of ours investigation topic is based mainly in the Model OSI and the Protocol TCP/IP.

Based on that exposed previously we guide the study and application of the project toward the Routers, their functions, benefits and types, as starting points toward the computer Security.

The Chapter II contain the whole Methodology of the Investigation, laid the foundation in the indicators hurtled by the application of the Dependent and Independent Variables step it was given to the concepts for the application of the different Techniques of Investigation (experimentation, field observation), as well as for the gathering of data (you interview interviews), later on you arrived to the main conclusions and agreement recommendations with the necessary requirements to fulfill the objective of our investigation work

In order to increase the viability of obtaining an appropriate utility, the development of the Thesis is based on a convenient one modeling of the analysis and design, it means it that during the Configuration of the Router they have space the prototypes of Rational Rose for the modeling of the design UML, the modern tools of interactive simulation for Routers CISCO the same one that offers an excellent atmosphere to examine alternating methods quickly, and usually voucher the pain to dedicate time to the design for the code.

In the Chapter III is the Proposal of the Thesis of Grade where the whole operative documentation is included for the use of Router CISCO 2811 of the CEYPSA to be adopted by the users of the same one, based mainly on the use and application of necessary operative tools for the application like the installation of the SDM that it allows the configuration in graphic way of the team (Router and Security Device Manager SDM) and the acondicionamiento for the installation of Java of Java Sun Microsystem

Finally we have the manual of user of the Router CISCO2811 of the CEYPSA the same one that fulfills the requirements of the administrators and users of the Net of Data extensively. As for the conformity and covering of the necessities of the Router, it satisfies in a clear way the Administrator's expectations with the following parameters:

- They show a standard method for the security of the information
- They possess control to administer the Router
- They maintain a communication mechanism between the processes and the software
- They enjoy graphic visualization of the control of the Router.

## INTRODUCCION

El desarrollo mismo del proceso educativo al interior de la Universidad Técnica de Cotopaxi es cada vez más exigente en el manejo de Tecnologías de Información y Comunicación (TIC's), por cuanto se requiere de la utilización de redes conectadas al Internet. El manejo de los sistemas administrativos, escolásticos y financieros implementados en el Centro de Experimentación y Producción Salache amerita que la información sea manejada en forma integral por todas las dependencias inmersas en la labor educativa, sobre todo aquella referente a datos personales de los estudiantes, información socioeconómica, record académico, control de asistencia, entre otros. Desafortunadamente las intrusiones en redes por parte de usuarios externos e internos se han convertido en un suceso habitual, lo que significa que las organizaciones deben instalar alguna protección contra las mismas.

Por esta razón el grupo de investigación ha pensado que el presente trabajo ha de contribuir con la seguridad de la información basados en la capacidad de los Routers para discriminar entre paquetes y restringirlos en sus puertos con base en criterios específicos de protocolo así como la toma de decisiones basándose en tablas de datos y reglas, por medio de filtros, a fin de que sólo la información de una cierta dirección puedan pasar a través de la Red de Datos del CEYPSA. En este momento la seguridad no es un lujo, es un requisito.

En el desarrollo de este proyecto se dan los pasos necesarios para establecer un nivel óptimo de seguridad en la Red de Datos del CEYPSA-UTC; este documento contiene información, instrucciones así como los procedimientos pertinentes a todos los trabajos de operación mantenimiento y modificación de configuraciones del Router CISCO 2811 del CEYPSA. Todo su contenido ha sido elaborado teniendo en cuenta las necesidades observadas en la Red de Datos del CEYPSA. La información precisada se halla establecida en función de varios programas de muestreo aplicados por el grupo investigador, basados en publicaciones emitidas

por la Compañía Cisco Systems así como en varias organizaciones gubernamentales y privadas que basan el flujo de sus Redes en Routers Cisco.

# **CAPITULO I**

## **TRANSMISIÓN DE DATOS**

### **1.1 Generalidades de transmisión de datos**

Según Microsoft ® Encarta ®, 2006 “Es la transmisión de información de un lugar a otro, tanto dentro de un ordenador o computadora”.

Según Julián Espinoza, 2002 “Es el envío de la información desde la unidad emisora a la receptora, los datos son transformados en señales dependientes del tipo que sean capaces de atravesar un medio y llegar al destino en las mejores condiciones”.

Según la Real Academia de la Lengua, 2006 “Transferir información de un lugar a otro mediante medios de transmisión”.

De lo anteriormente citado se indica que, transmisión de datos es el traslado de información de un lugar a otro mediante diferentes dispositivos de comunicación.

## **1.1.1 Tipos de Transmisión**

### **1.1.1.1 La transmisión analógica**

Es la unidad emisora que genera señales que originan diferencias de tensión entre los conductores de la línea. Estas variaciones son detectadas en la unidad receptora y transformadas por ésta en señales de partida.

### **1.1.1.2. La transmisión digital**

Se basa en la representación discreta de una señal, toma los valores fijos y definidos, por lo que para recibirla es suficiente con saber si llega o no la señal.

Últimamente se utiliza mucho la transmisión digital debido a que:

- La tecnología digital se ha abaratado mucho.
- Al usar repetidores en vez de amplificadores, el ruido y otras distorsiones no es acumulativo.
- La utilización de banda ancha es más aprovechada por la tecnología digital.
- Los datos transportados se pueden encriptar y por tanto hay más seguridad en la información.
- Al tratar digitalmente todas las señales, se pueden integrar servicios de datos analógicos (voz, video, etc...) con digitales como texto y otros.

## **1.1.2 Medios de Transmisión Guiados**

En medios guiados, el ancho de banda o velocidad de transmisión dependen de la distancia y de si el enlace es punto a punto o multipunto. Los cuales se describen a continuación:

### **1.1.2.1 Par trenzado**

Es el medio guiado más barato y más usado, consiste en un par de cables, embutidos para su aislamiento, para cada enlace de comunicación. Debido a que puede haber acoples entre pares, estos se trenza con pasos diferentes. La utilización del trenzado tiende a disminuir la interferencia electromagnética.

Este tipo de medio es el más utilizado debido a su bajo coste (se utiliza mucho en telefonía) pero su inconveniente principal es su poca velocidad de transmisión y su corta distancia de alcance. Con estos cables, se pueden transmitir señales analógicas o digitales. Es un medio muy susceptible a ruido y a interferencias. Para evitar estos problemas se suele trenzar el cable con distintos pasos de torsión y se suele recubrir con una malla externa para evitar las interferencias externas.

### **1.1.2.2 Pares trenzados apantallados y sin apantallar**

Los pares sin apantallar son los más baratos aunque los menos resistentes a interferencias (aunque se usan con éxito en telefonía y en redes de área local). A velocidades de transmisión bajas, los pares apantallados son menos susceptibles a interferencias, aunque son más caros y más difíciles de instalar.

### **1.1.2.3 Cable coaxial**

Consiste en un cable conductor interno (cilíndrico) separado de otro cable conductor externo por anillos aislantes o por un aislante macizo. Todo esto se recubre por otra capa aislante que es la funda del cable. Este cable, aunque es más caro que el par trenzado, se puede utilizar a más larga distancia, con velocidades de transmisión superiores, menos interferencias y permite conectar más estaciones.

Se utiliza para transmitir señales analógicas o digitales. Sus inconvenientes principales son: atenuación, ruido térmico, ruido de intermodulación. Para señales analógicas, se necesita un amplificador cada pocos kilómetros y para señales digitales un repetidor cada kilómetro.

### **1.1.2.4 Fibra óptica:**

Se trata de un medio muy flexible y muy fino que conduce energía de naturaleza óptica, su forma es cilíndrica con tres secciones radiales: núcleo, revestimiento y cubierta.

El núcleo está formado por una o varias fibras muy finas de cristal o plástico. Cada fibra está rodeada por su propio revestimiento que es un cristal o plástico con diferentes propiedades ópticas distintas a las del núcleo. Alrededor de este conglomerado está la cubierta (constituida de material plástico o similar) que se encarga de aislar el contenido de aplastamientos, abrasiones, humedad entre otros.

Es un medio muy apropiado para largas distancias e incluso últimamente para LAN's. Sus beneficios frente a cables coaxiales y pares trenzados son:

- Permite mayor ancho de banda.
- Menor tamaño y peso.
- Menor atenuación.
- Aislamiento electromagnético.
- Mayor separación entre repetidores.

## **1.2. Redes Informáticas**

Según Microsoft ® Encarta ® ,2006 “Es un conjunto de técnicas, conexiones físicas y programas informáticos empleados para conectar dos o más ordenadores o computadoras. Los usuarios de una red pueden compartir ficheros, impresoras y otros recursos, enviar mensajes electrónicos y ejecutar programas en otros ordenadores”.

Según la Real Academia de la Lengua, 2006 “Infraestructura de cable que permite la interconexión entre los ordenadores ya sea a nivel local, nacional o mundial”.

Desde el punto de vista de M.Schwartz (2000), “Es la comunicación interna dentro de una empresa permitiendo compartir recursos y apertura hacia el exterior es decir hacia otras redes locales o hacia redes públicas”

De lo citado se puede inferir que, una red informática es la unión de dos o más computadoras, donde permite que varios usuarios puedan acceder a recursos y dispositivos determinados.

Una red tiene tres niveles de componentes

- Software de aplicaciones.
- Software de red
- Hardware de red.

### **1.2.1 Software de aplicaciones**

Está formado por programas informáticos que se comunican con los usuarios de la red y permiten compartir información (como archivos de bases de datos, de documentos, gráficos o videos) y recursos (como impresoras o unidades de disco).

Un tipo de software de aplicaciones se denomina cliente-servidor. Las computadoras cliente envían peticiones de información o de uso de recursos a otras computadoras, llamadas servidores, que controlan el flujo de datos y la ejecución de las aplicaciones a través de la red. Otro tipo de software de aplicación se conoce como “de igual a igual” (peer to peer). En una red de este tipo, los ordenadores se envían entre sí mensajes y peticiones directamente sin utilizar un servidor como intermediario.

Estas redes son más restringidas en sus capacidades de seguridad, auditoría y control, y normalmente se utilizan en ámbitos de trabajo con pocos ordenadores y

en los que no se precisa un control tan estricto del uso de aplicaciones y privilegios para el acceso y modificación de datos; se utilizan, por ejemplo, en redes domésticas o en grupos de trabajo dentro de una red corporativa más amplia.

### **1.2.2. Software de red**

Consiste en programas informáticos que establecen protocolos, o normas, para que las computadoras se comuniquen entre sí. Estos protocolos se aplican enviando y recibiendo grupos de datos formateados denominados paquetes. Los protocolos indican cómo efectuar conexiones lógicas entre las aplicaciones de la red, dirigir el movimiento de paquetes a través de la red física y minimizar las posibilidades de colisión entre paquetes enviados simultáneamente.

### **1.2.3. Hardware de red**

Está formado por los componentes materiales que unen las computadoras. Dos componentes importantes son los medios de transmisión que transportan las señales de los ordenadores (típicamente cables estándar o de fibra óptica, aunque también hay redes sin cables que realizan la transmisión por infrarrojos o por radiofrecuencias) y el adaptador de red, que permite acceder al medio material que conecta a los ordenadores, recibir paquetes desde el software de red y transmitir instrucciones y peticiones a otras computadoras. La información se transfiere en forma de dígitos binarios, o bits (unos y ceros), que pueden ser procesados por los circuitos electrónicos de los ordenadores.

Las redes informáticas proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro, todos los archivos podrían duplicarse en dos o tres

máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias. Además, la presencia de múltiples CPU significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque se tenga un rendimiento global menor.

Los beneficios que presentan las redes, son en los ordenadores pequeños tienen una mejor relación costo / rendimiento, comparada con la ofrecida por las máquinas grandes. Estas son, a grandes rasgos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es miles de veces mayor. Este desequilibrio ha ocasionado que muchos diseñadores de sistemas construyan sistemas constituidos por poderosos ordenadores personales, uno por usuario, con los datos guardados una o más máquinas que funcionan como servidor de archivo compartido. EL establecimiento de una red de ordenadores, es que puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre sí.

### **1.3. Topología de las Redes**

Según Julián Espinoza, 2002 “Es la composición o forma física de ordenadores, cables y otros componentes en la red, donde se lleva a cabo la conexión”.

Según Microsoft ® Encarta ® ,2006 “Es la configuración adoptada por las estaciones de trabajo para conectarse entre sí, esto permite organizar las computadoras de una red”.

Según la Real Academia de la Lengua, (2006) “Es la disposición de diferentes componentes de una red, la topología idónea para una red concreta depende del

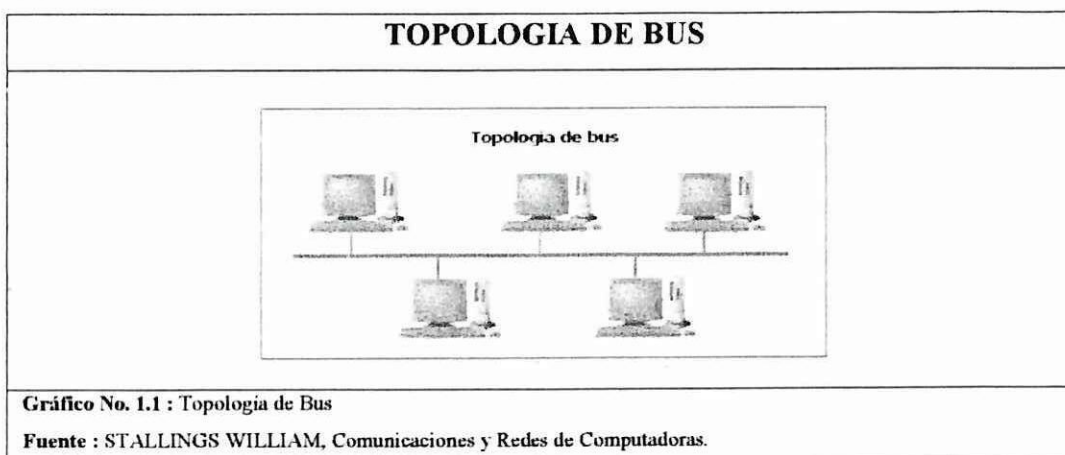
número de máquinas a interconectar y el tipo de acceso al medio físico que deseemos”.

De lo anteriormente mencionado se puede inferir que, Topología de redes son los diferentes componentes que van a formar parte de una red se pueden interconectar o unir de diferentes formas, siendo la forma elegida un factor fundamental que va a determinar el rendimiento y la funcionalidad de la red. Las principales topologías son:

### **1.3.1. Topología de Bus**

Tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente, aunque la ruptura del cable hace que los hosts queden desconectados. La topología de bus permite que todos los dispositivos de la red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si desea que todos los dispositivos obtengan esta información. Es la topología más común en pequeñas LAN, con hub o switch final en uno de los extremos, (Gráfico No.1.1)

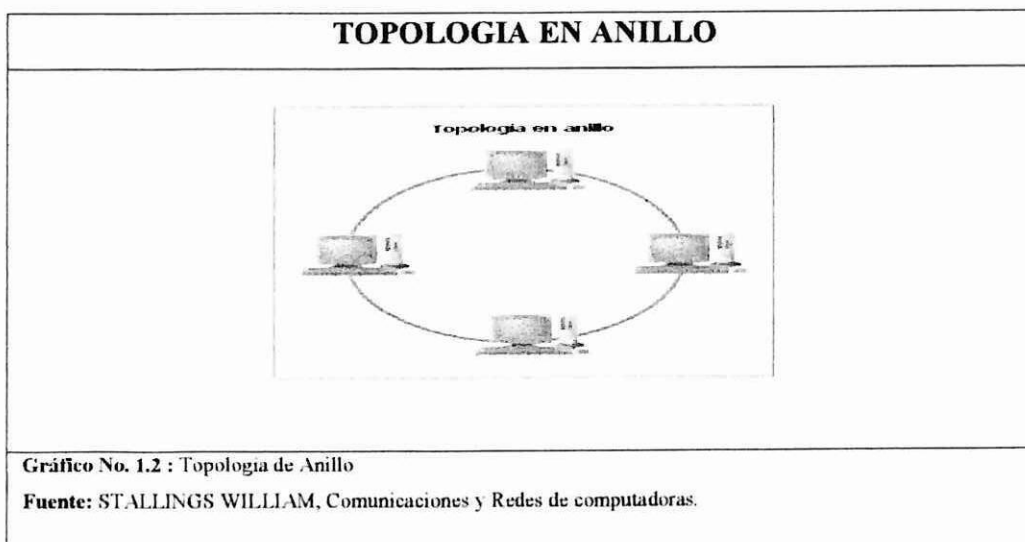
Gráfico No. 1.1



### 1.3.2. Topología de Anillo

Se compone de un solo anillo cerrado formado por nodos y enlaces, en el que cada nodo está conectado solamente con los dos nodos adyacentes. Los dispositivos se conectan directamente entre sí por medio de cables en lo que se denomina una cadena margarita. Para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.

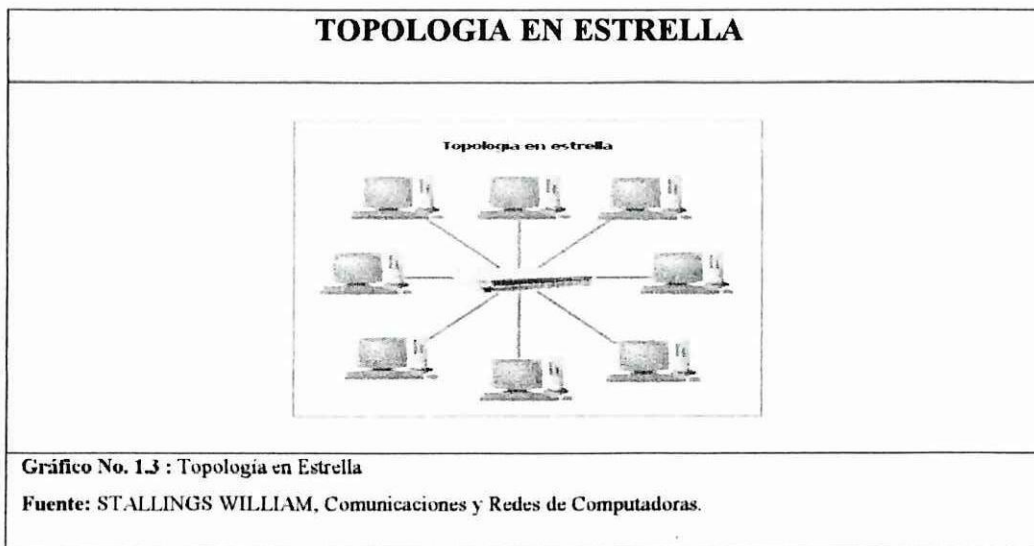
Gráfico No. 1.2



### 1.3.3. Topología en Estrella

Tiene un nodo central desde el que se irradian todos los enlaces hacia los demás nodos. Por el nodo central, generalmente ocupado por un concentrador, pasa toda la información que circula por la red. La ventaja principal es que permite que todos los nodos se comuniquen entre sí de manera conveniente. La desventaja principal es que si el nodo central falla, toda la red se desconecta.

Gráfico No. 1.3



### 1.4. Tipos de redes

Según la pagina web <http://www.solont.com/>, (2007) “Son clases de redes que depende de la cobertura geográfica”.

Según Microsoft ® Encarta ® ,2006 “Son clasificaciones de las redes dependiendo del espacio geográfico donde se ubique, estas utilizan tecnología de transmisión ”.

Según Julián Espinoza, 2002 “Son categorías que dependen de una gran variedad de redes no sólo por el número sino también por la diversidad de protocolos que ellas utilizan”.

De lo citado anteriormente se puede decir que los tipos de redes son clasificaciones de las diferentes redes que existan en un determinado lugar.

Según Las redes de acuerdo a la cobertura geográfica pueden ser clasificadas en LAN, MAN, WAN.

#### **1.4.1 LAN (Local Área Network): Redes de Área Local**

Es un sistema de comunicación entre computadoras que permite compartir información, con la característica de que la distancia entre las computadoras debe ser pequeña. Estas redes son usadas para la interconexión de computadores personales y estaciones de trabajo. Se caracterizan por: tamaño restringido, tecnología de transmisión (por lo general broadcast), alta velocidad y topología. Son redes con velocidades entre 10 y 100 Mbps, tiene baja latencia y baja tasa de errores. Cuando se utiliza un medio compartido es necesario un mecanismo de arbitraje para resolver conflictos.

#### **1.4.2 MAN (Metropolitan Area Network): Redes de Área Metropolitana**

Es una versión de mayor tamaño de la red local. Puede ser pública o privada. Una MAN puede soportar tanto voz como datos. La razón principal para distinguirla de otro tipo de redes, es que para las MAN's se ha adoptado un estándar llamado DQDB (Distributed Queue Dual Bus) o IEEE 802.6. Utiliza medios de difusión al igual que las Redes de Área Local.

#### **1.4.3 WAN (Wide Area Network): Redes de Amplia Cobertura**

Son redes que cubren una amplia región geográfica, a menudo un país o un continente. Este tipo de redes contiene máquinas que ejecutan programas de usuario llamadas hosts o sistemas finales (end system).

En la mayoría de las redes de amplia cobertura se pueden distinguir dos componentes: Las líneas de transmisión y los elementos de intercambio (conmutación). Las líneas de transmisión se conocen como circuitos, canales o troncales. Los elementos de intercambio son computadores especializados utilizados para conectar dos o más líneas de transmisión.

### **1.5. Modelos de Comunicación**

Según Microsoft ® Encarta ® ,2006 “Son estándares que permite intercambiar información entre varios sistemas”.

Según Julián Espinoza, 2002 “Es un proceso donde permite enviar los datos desde un ordenador a otro, este procedimiento puede ser roto en tareas discretas como reconocer, dividir y añadir datos”.

Según la pagina web <http://www.solont.com/> , (2007) “Son arquitecturas que divide las comunicaciones de red en varios niveles conformadas por capas”.

De lo citado podemos inferir que los modelos de comunicación son arquitecturas donde identifican la forma en la que se realiza el complejo proceso de enviar datos por una red.

Las dos arquitecturas de redes más importantes son, en la actualidad, las correspondientes a los protocolos OSI y TCP/IP. Generalmente para cada capa de una arquitectura determinada existirá uno o varios protocolos, y para protocolo habrá múltiples implementaciones.

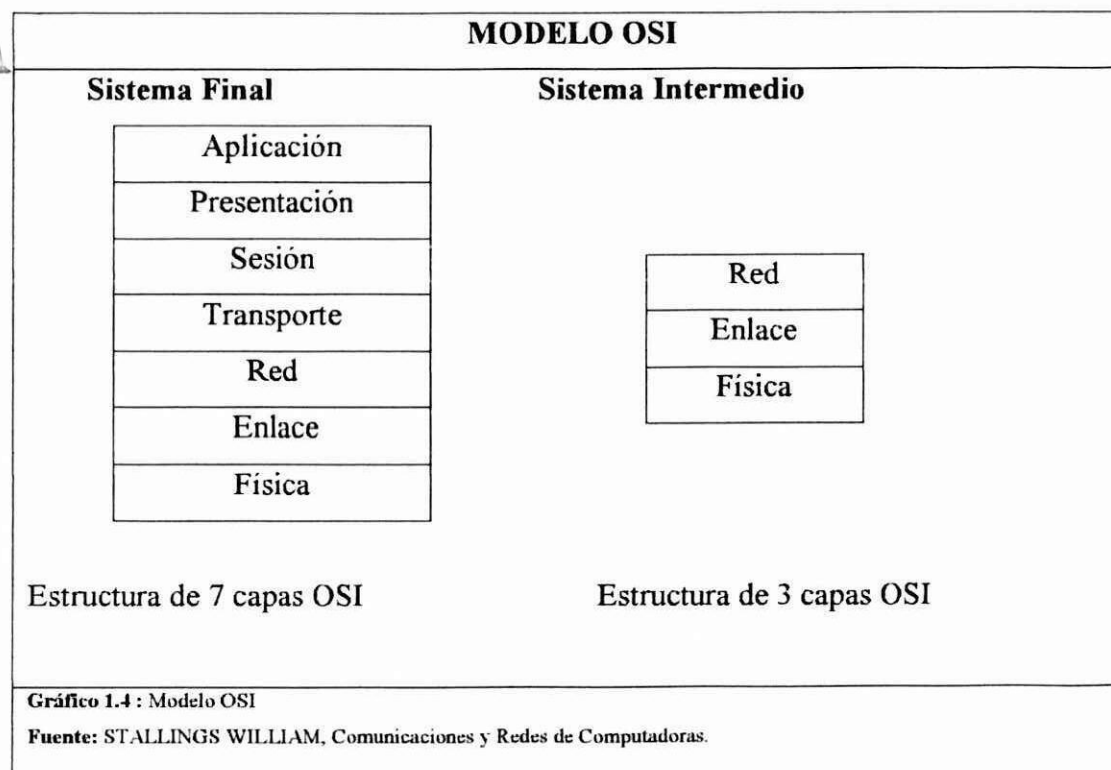
### **1.5.1 Modelo OSI**

OSI (International Organization for Standardization), estuvo creando y definiendo hasta el año 1983 una arquitectura de redes denominada OSI, El sistema de comunicaciones del modelo OSI realiza una estructura del proceso en varias capas que interaccionan entre sí.

El Modelo consiste en que una capa determinada proporciona servicios a la capa superior contigua toma los servicios que le presenta la siguiente capa inferior.

De esta manera, las tareas se pueden dividir en otras a su vez más pequeñas y por tanto más manejables. La propuesta OSI fue la siguiente: Para un terminal o host propusieron una estructura de 7 y 3 capas como puede apreciarse.

Gráfico 1.4



## 1.6.- Protocolos de comunicación

Según Microsoft ® Encarta ® ,2006 “Es el procedimiento que se utiliza para mover la información de una localización a otra sin errores”.

Según Gustavo Rueda, (2000) “Es el conjunto de reglas previamente establecidas que definen los procedimientos para que dos o más procesos intercambien

información. Estas definen la sintaxis, la semántica y la sincronización del protocolo”.

Según Julián Espinoza, (2000) “Es un conjunto de reglas que controla la comunicación”.

De lo anteriormente mencionado podemos citar que, protocolo de comunicación es un conjunto de procedimientos establecidos que definen procedimientos.

### **1.6.1 Características**

Un protocolo es el conjunto de normas para comunicarse dos o más entidades (objetos que se intercambian información). Los elementos que definen un protocolo son:

- Sintaxis: formato, codificación y niveles de señal de datos.
- Semántica: información de control y gestión de errores.
- Temporización: coordinación entre la velocidad y orden secuencial de las señales.

Las características más importantes de un protocolo son:

- Directo/indirecto: los enlaces punto a punto son directos pero los enlaces entre dos entidades en diferentes redes son indirectos ya que intervienen elementos intermedios.
- Monolítico/estructurado: monolítico es aquel en que el emisor tiene el control en una sola capa de todo el proceso de transferencia. En protocolos estructurados, hay varias capas que se coordinan y que dividen la tarea de comunicación.
- Simétrico/asimétrico: los simétricos son aquellos en que las dos entidades que se comunican son semejantes en cuanto a poder tanto emisores como consumidores de información. Un protocolo es asimétrico si una de las entidades tiene funciones diferentes de la otra ( por ejemplo en clientes y servidores ) .
- Normalizado/no normalizado: los no normalizados son aquellos creados específicamente para un caso concreto y que no va a ser necesario conectarlos con agentes externos. En la actualidad, para poder intercomunicar muchas entidades es necesaria una normalización.

### 1.6.2 Funciones

- Segmentación y ensamblado: generalmente es necesario dividir los bloques de datos en unidades pequeñas e iguales en tamaño, y este proceso se le llama segmentación. El bloque básico de segmento en una cierta capa de un protocolo se le llama PDU (Unidad de datos de protocolo). La necesidad de la utilización de bloque es por :
  - La red sólo admite la transmisión de bloques de un cierto tamaño.
  - El control de errores es más eficiente para bloques pequeños.
  - Para evitar monopolización de la red para una entidad, se emplean bloques pequeños y así una compartición de la red.

- Con bloques pequeños las necesidades de almacenamiento temporal son menores.
- Encapsulado: se trata del proceso de adherir información de control al segmento de datos. Esta información de control es el direccionamiento del emisor/receptor, código de detección de errores y control de protocolo.
- Control de conexión: hay bloques de datos sólo de control y otros de datos y control. Cuando se utilizan datagramas, todos los bloques incluyen control y datos ya que cada PDU se trata como independiente. En circuitos virtuales hay bloques de control que son los encargados de establecer la conexión del circuito virtual. Hay protocolos más sencillos y otros más complejos, por lo que los protocolos de los emisores y receptores deben de ser compatibles al menos .Además de la fase de establecimiento de conexión (en circuitos virtuales) está la fase de transferencia y la de corte de conexión . Si se utilizan circuitos virtuales habrá que numerar los PDU y llevar un control en el emisor y en el receptor de los números.
- Entrega ordenada: el envío de PDU puede acarrear el problema de que si hay varios caminos posibles, lleguen al receptor PDU desordenados o repetidos, por lo que el receptor debe de tener un mecanismo para reordenar los PDU. Hay sistemas que tienen un mecanismo de numeración con módulo algún número; esto hace que el módulo sean lo suficientemente alto como para que sea imposible que haya dos segmentos en la red al mismo tiempo y con el mismo número.
- Control de flujo: hay controles de flujo de parada y espera o de ventana deslizante. El control de flujo es necesario en varios protocolos o capas, ya que el problema de saturación del receptor se puede producir en cualquier capa del protocolo .
- Control de errores: generalmente se utiliza un temporizador para retransmitir una trama una vez que no se ha recibido confirmación después de expirar el tiempo del temporizador. Cada capa de protocolo debe de tener su propio control de errores.
- Direccionamiento: cada estación o dispositivo intermedio de almacenamiento debe tener una dirección única. A su vez, en cada terminal o sistema final

puede haber varios agentes o programas que utilizan la red, por lo que cada uno de ellos tiene asociado un puerto.

- Además de estas direcciones globales, cada estación o terminal de una subred debe de tener una dirección de subred (generalmente en el nivel MAC).
- Hay ocasiones en las que se usa un identificador de conexión; esto se hace así cuando dos estaciones establecen un circuito virtual y a esa conexión la numeran (con un identificador de conexión conocido por ambas). La utilización de este identificador simplifica los mecanismos de envío de datos ya que por ejemplo es más sencillo que el direccionamiento global.
- Algunas veces se hace necesario que un emisor emita hacia varias entidades a la vez y para eso se les asigna un direccionamiento similar a todas.
- Multiplicación: es posible multiplexar las conexiones de una capa hacia otra, es decir que de una única conexión de una capa superior, se pueden establecer varias conexiones en una capa inferior (y al revés).
- Servicios de transmisión: los servicios que puede prestar un protocolo son:
  - Prioridad
  - Grado de servicio
  - Seguridad.

### **1.6.3. Tipos de Protocolos**

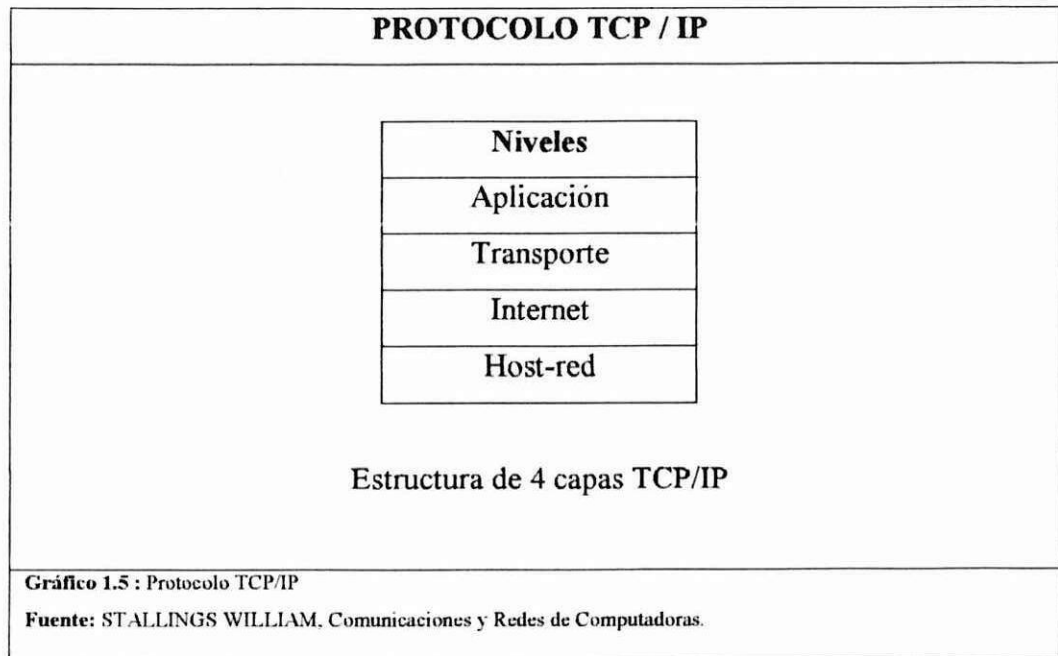
Existen más de 100 protocolos diferentes definidos en este conjunto. Para nuestra investigación solo tomaremos el TCP/IP.

### **1.6.4 Protocolo TCP/IP**

El nombre TCP/IP Proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). Es la base del

Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, mini computadoras y computadoras centrales sobre redes de área local y área extensa. Este protocolo se compone únicamente de cuatro capas.

Gráfico 1.5



## 1.7.- Router

Según Julián Espinoza “Es un elemento en una red cuya función es el encaminamiento del tráfico que le llega hasta los terminales de destino, por una ruta lo más apropiado y rápida posible”.

Según Gustavo Rueda, (2000) “Son dispositivos electrónicos complejos que permite manejar comunicaciones entre redes “.

De lo manifestado anteriormente, se puede decir que un Router es el camino de un elemento más inteligente y posibilita la interconexión de diferentes tipos de redes de ordenadores.

Según Microsoft ® Encarta ® ,2006 “Es un dispositivo de propósito general diseñado para segmentar la red, con la idea de limitar tráfico de broadcast y proporcionar seguridad, control y redundancia entre dominios individuales de broadcast”.

Por cada red a la que está conectado, dispondrá de un interfaz de red y su correspondiente IP. Lo que diferencia un Router de otro equipo con varios interfaces es que el Router hace IP-FORWARD (ip- hacia adelante) de paquetes, esto es, si por un interfaz llega un paquete cuyo destino es un host conectado a otra red, y se tiene un camino hacia ese host a través de algún otro interfaz, el Router propagara ese paquete por el otro interfaz.

### **1.7.1. Funciones de un ruteador**

Las funciones primarias de un ruteador son:

- Segmentar la red dentro de dominios individuales de broadcast.
- Suministrar un envío inteligente de paquetes.
- Soportar rutas redundantes en la red.

- Aislar el tráfico de la red ayuda a diagnosticar problemas, puesto que cada puerto del ruteador es una subred separada, el tráfico de los broadcast no pasaran a través del ruteador.

### 1.7.2. Beneficios del Ruteador

- Proporcionar seguridad a través de sofisticados filtros de paquetes, en ambiente LAN y WAN.
- Consolidar el legado de las redes de mainframe IBM, con redes basadas en PCs a través del uso de Data Link Switching (DLSw).
- Permitir diseñar redes jerárquicas, que deleguen autoridad y puedan forzar el manejo local de regiones separadas de redes internas.
- Integrar diferentes tecnologías de enlace de datos, tales como Ethernet, Fast Ethernet, Token Ring, FDDI y ATM.

### 1.7.3.-Tipos de Router

Los tipos principales de Router son:

- **Estático.** Los Router estáticos requieren un administrador para generar y configurar manualmente la tabla de encaminamiento y para especificar cada ruta.
- **Dinámico.** Los Router dinámicos se diseñan para localizar, de forma automática, rutas y, por tanto, requieren un esfuerzo mínimo de

instalación y configuración. Son más sofisticados que los Router estáticos, examinan la información de otros Router y toman decisiones a nivel de paquete sobre cómo enviar los datos a través de la red.

#### 1.7.4.-Características de los dos tipos de Router

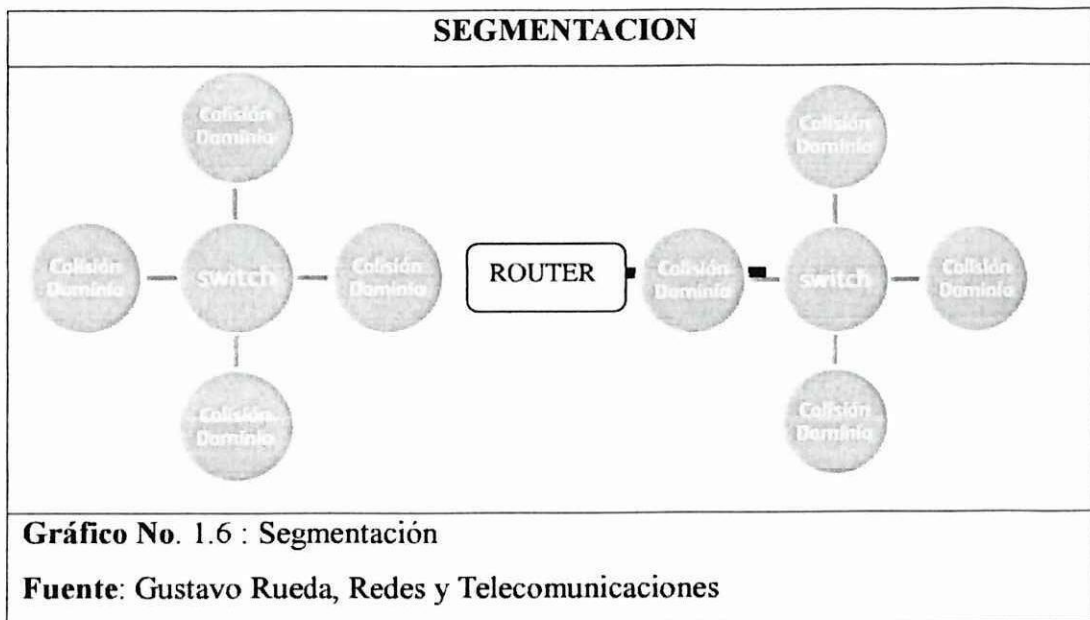
Tabla No. 1.1

<b>TIPOS DE ROUTER</b>	
<b>Router estáticos</b>	<b>Router dinámicos</b>
Instalación y configuración manual de todos los Router	Configuración manual del primer Router. Detectan automáticamente redes y Router adicionales
Utilizan siempre la misma ruta, determinada a partir de una entrada en la tabla de encaminamiento	Pueden seleccionar un ruta en función de factores tales como coste y cantidad del tráfico de enlace
Utilizan una ruta codificada (designada para manejar sólo una situación específica), no necesariamente la ruta más corta.	Pueden decidir enviar paquetes sobre rutas alternativas
Se consideran más seguros puesto que los administradores especifican cada ruta	Pueden mejorar la seguridad configurando manualmente el Router para filtrar direcciones específicas de red y evitar el tráfico a través estas direcciones
<p><b>Tabla No. 1.1 :</b> Tipos de Router  <b>Fuente:</b> STALLENGS WILLIAM, Comunicaciones y Redes de Computadoras.</p>	

## 1.7.5 Segmentado de Subredes con Routers

Un Router está diseñado para interconectar y definir los límites de los dominios de broadcast. La segmentación de la red con un Router en dos dominios diferentes de broadcast, en este medio el tráfico generado de broadcast no fluye a través del Router al otro dominio.

Gráfico No. 1.6



## 1.8. Seguridad informática

Según Randall K. Nichols, (2003) “Es la combinación de procesos, procedimientos y sistemas utilizados para garantizar la confidencialidad, la integridad o la disponibilidad de la información.

Según Microsoft ® Encarta ® ,2006 “Es la agrupación de procesos que permite garantizar la información donde los objetos deben permanecer accesibles a entidades autorizadas y verificar la identidad del emisor y del receptor.

Según Gustavo Rueda, (2000) “Es la unión de procedimientos que sirven para garantizar la confiabilidad de la información”.

De lo anteriormente manifestado, podemos inferir que seguridad informática es un procedimiento que permite garantizar la información, los objetos deben ser modificados por entidades autorizadas y de manera controlada.

Los tres elementos que se deben proteger son el hardware (servidor, cableado, etc.), el software (sistema operativo, aplicaciones, etc.) y los datos (documentos, bases de datos, etc.). Las amenazas a las que pueden estar expuestos estos elementos son:

- **Interrupción:** Un recurso del sistema es destruido o se vuelve no disponible. También es denominado Negación de Servicio.
- **Intercepción:** Una entidad no autorizada consigue acceso a un recurso.
- **Modificación:** Una entidad no autorizada no solo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad.
- **Fabricación:** Una entidad no autorizada inserta objetos falsificados en el sistema.

## **1.8.1 Mecanismos de Seguridad**

Los mecanismos de seguridad se dividen en tres grupos:

### **1.8.1.1 Prevención**

Aquellos que aumentan la seguridad de un sistema durante su funcionamiento normal.

- Control de enrutamiento
- Unicidad
- Gestión de claves

### **1.8.1.2 Detección**

Aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación.

- Firewalls
- Filtrado de Paquetes
- Monitoreo de la Actividad

### **1.8.1.3 Recuperación**

Aquellos que se aplican cuando el sistema ha sido atacado.

- Cifrado
- Tráfico de relleno
- Proxy de Aplicación

## **1.8.2 Servidor de Seguridades**

Un servidor de seguridad personal se define como un servicio de software que se ejecuta en un sistema operativo que proporciona una sencilla funcionalidad de servidor de seguridad para un equipo personal. Al crecer el número de conexiones permanentes a Internet (al contrario que las conexiones de acceso telefónico), ha aumentado el uso de servidores de seguridad personales.

Aunque se ha diseñado para proteger a un único equipo personal, un servidor de seguridad personal también puede proteger a una red pequeña si el equipo en el que se ha instalado comparte su conexión a Internet con otros equipos de la red interna. Sin embargo, un servidor de seguridad personal tiene un rendimiento limitado y reduce el rendimiento del equipo personal en el que está instalado. Los mecanismos de protección suelen ser menos efectivos que una solución de servidor de seguridad dedicada porque suelen estar restringidos al bloqueo de direcciones IP y de puertos aunque, en general, un equipo personal necesita un nivel de protección inferior.

### **1.8.2.1. Características del servidor de seguridad**

En función de las características que admita un servidor de seguridad, el tráfico se permite o bloquea mediante varias técnicas. Dichas técnicas ofrecen grados distintos de protección, según las capacidades del servidor de seguridad. Las características siguientes del servidor de seguridad se enumeran de menor a mayor complejidad:

- Filtros de entrada del adaptador de red
- Filtros de paquetes estáticos
- Traducción de direcciones de red (NAT)
- Inspección con estado
- Inspección de circuitos
- Filtrado de aplicaciones

### **1.8.2.2 Clases de servidor de seguridad**

Las clases de servidor de seguridad específicas pueden utilizarse para responder a requisitos específicos del diseño de una arquitectura de TI. La agrupación de servidores de seguridad en clases permite la abstracción del hardware de los requisitos del servicio. A continuación, pueden hacerse coincidir los requisitos del servicio con las características de la clase. Siempre que un servidor de seguridad encaje en una clase específica, éste puede admitir todos los servicios que se requiere que admita la clase. Las clases son las siguientes:

- Clase 1: Servidores de seguridad personales
- Clase 2: Servidores de seguridad de enrutador
- Clase 3: Servidores de seguridad de hardware inferiores

- Clase 4: Servidores de seguridad de hardware superiores
- Clase 5: Servidores de seguridad de servidor superiores

## **CAPITULO II**

# **METODOLOGÍA DE LA INVESTIGACIÓN**

### **2.1. Introducción**

La extensión de las redes de ámbito mundial que interconectan recursos informáticos ha hecho que los peligros que sufre la información almacenada en los diversos sistemas crezcan considerablemente y se diversifiquen, y que las medidas adoptadas internamente sean insuficientes frente a mayores formas de ataque a la seguridad en red, incluyendo los virus, Caballos de Troya y penetración de las redes internas.

A raíz de la interconexión del mundo a la Internet, viaja por ella y se almacena información de todo tipo, que abarca desde noticias, documentos, normas y aplicaciones informáticas de libre distribución hasta complejas transacciones que requieren medidas que garanticen la confidencialidad, la integridad y el origen de los datos. Los procedimientos de escucha electrónica y los sabotajes realizados tanto por atacantes externos como internos, están causando últimamente la pérdida de grandes cantidades de información.

Los recursos de hardware especializado son designados para recibir solicitudes anónimas de una manera rápida y eficiente desde distintos puntos del mundo en la Internet. De tal forma, ellos proveen un portal que puede ser usado por amigos y enemigos igualmente. Por su naturaleza, son recursos especializados que demandan un alto nivel de seguridad. El tipo de tecnología que mejor cumple con estas demandas es el Router.

Por esta razón el grupo de investigación ha pensado que el presente trabajo ha de contribuir con la seguridad de la información, para controlar el tráfico que pasa directamente entre las redes a fin de que se pueda proporcionar un mecanismo poderoso de direccionamiento y por lo tanto restringir servicios que pueden poner en peligro la seguridad de la información del Centro Experimental y Producción Salache (CEYPSA) de la Universidad Técnica de Cotopaxi.

De la misma manera, basados en la capacidad de los Routers para discriminar entre paquetes y restringirlos en sus puertos con base en criterios específicos de protocolo se va a proceder con tácticas de filtración de paquetes, así como la toma de decisiones basándose en tablas de datos y reglas, por medio de filtros, a fin de que sólo datos de una cierta dirección puedan pasar a través del Ruteador del CEYPSA.

En el desarrollo de este proyecto, se darán los pasos necesarios para establecer un nivel óptimo de seguridad en la red de datos del Centro Experimental y Producción Salache (CEYPSA) de la Universidad, que enseñará al personal encargado a tomar este tema como uno de los puntos claves para el buen funcionamiento del sistema. En este momento, la seguridad no es un lujo es un requisito.

## 2.2. Población a Investigar

El presente estudio investigativo se llevará a cabo en la Provincia de Cotopaxi, cantón Latacunga en Centro Experimental y Producción Salache. Para el cálculo de estos parámetros se toma en cuenta a los encargados de las áreas designadas por la red de datos del CEYPSA, por cuanto son ellos los que administran los recursos tecnológicos y operativos de los usuarios finales de la UTC que utilizan la red de datos. El Universo de proyección estimativa es de 17 usuarios que están distribuidos de la siguiente manera:

Tabla No. 2.1

<b>POBLACION</b>	
<b>Departamentos</b>	<b>N. Personal</b>
Direcciones de Carrera	2
Área Administrativa	4
Departamento de Servicios Informáticos	5
Laboratorios	6
<b>TOTAL</b>	<b>17</b>
Tabla No 2.1: (Población )	
Fuente: Grupo Investigador	

Debido a que la población no es superior de 100 usuarios para la muestra se seleccionara toda la población.

## 2.3. Operacionalización de las variables

### 2.3.1 Variable Independiente

Interpretación y conceptualización de requerimientos para la configuración de un Router en el CEYPSA-UTC

Tabla No. 2.2

VARIABLE INDEPENDIENTE			
CONCEPTUALIZACIÓN	INDICADORES	ITEMES BÁSICOS	TÉCNICAS
<p>La configuración se conceptualiza como:</p> <ul style="list-style-type: none"> <li>Router</li> </ul>	<ul style="list-style-type: none"> <li>Requerimientos de hardware</li> <li>Diagnóstico de la funcionalidad del Router</li> <li>Impacto del Router en la administración de la red de datos</li> <li>Disponibilidad de la Red</li> </ul>	<ul style="list-style-type: none"> <li>¿Conoce usted que es un Router?</li> <li>¿Sabía usted que un Router permite que el destino de la información llegue en forma rápida y segura?</li> <li>¿Piensa usted que un Router agilizaría el proceso de la información en el CEPSA?</li> <li>¿Piensa usted que los diferentes departamentos existentes que se encuentra en red con un Router tendrían una red disponible?</li> </ul>	<p>Encuesta</p> <p>Estructurada al personal que labora en los Departamentos, Direcciones, Centros y Oficinas del CEYPSA.</p>

Tabla No 2.2: Variable Independiente

Fuente: Investigadores

### 2.3.2 Variable Dependiente:

Optimizar la administración de la red de datos del Centro Experimental y Producción Salache (CEYPSA) de la Universidad Técnica de Cotopaxi.

Tabla No. 2.3

VARIABLE DEPENDIENTE			
CONCEPTUALIZACIÓN	INDICADORES	TEMAS BÁSICOS	TÉCNICAS
<p>La administración de la red de datos se conceptualiza como:</p> <ul style="list-style-type: none"> <li>• Optimización</li> <li>• Seguridad</li> </ul>	<ul style="list-style-type: none"> <li>• Planificación de la administración de la red de datos.</li> <li>• Servicios de red</li> <li>• Confabilidad del uso de Router en la administración de la red de datos.</li> </ul>	<ul style="list-style-type: none"> <li>• ¿Le molesta que su información se procese en forma insegura y lenta?</li> <li>• ¿Piensa usted que en el Departamento de Servicios Informáticos falta una planificación adecuada en el proceso de la información?</li> <li>• ¿Desearía usted que se implemente un Router en la red de datos del centro experimental y producción salache (CEYPSA) de la UTC?</li> <li>• ¿Cree usted que es importante que el CEYPSA, cuente con un Router en el Departamento de Servicios Informáticos?</li> </ul>	<p>Encuesta estructurada al personal que labora en los Departamentos, Direcciones, Centros y Oficinas del CEYPSA.</p>

Tabla No.2.3 Variable Dependiente

Fuente: Investigadores

## 2.4. Recolección y procesamiento de Datos

- Preparación de instrumentos (vea en anexos el Encuesta N°. 1.1).
- Afinamiento y aplicación de los instrumentos
- Los datos obtenidos serán puestos al proceso de limpiado, tabulado y codificado.
- Elaboración de cuadros
- Aplicación del diseño estándar apropiado por el cual nos permitirá verificar las hipótesis.
- Análisis e interpretación de datos, los mismos que se realizarán de manera cualitativa y cuantitativa.
- Análisis y construcción de los resultados.
- Conclusiones y recomendaciones

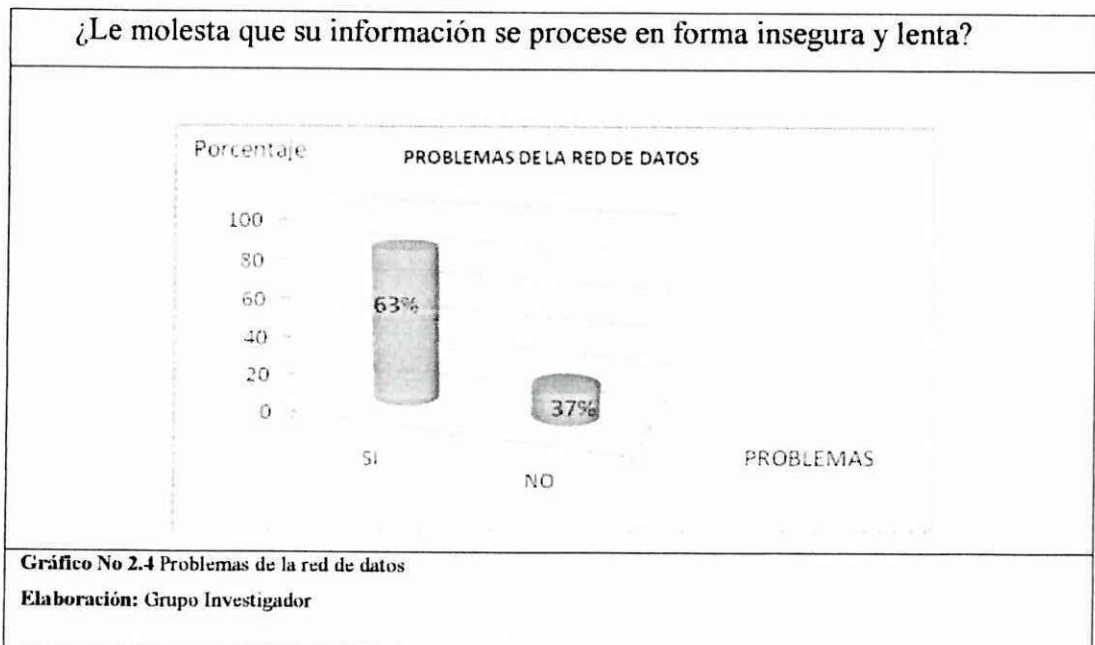
## 2.4.1. Presentación y análisis de resultados

Tabla No. 2.4

¿Le molesta que su información se procese en forma insegura y lenta?	
Problemas con la red de Datos	Porcentaje (%)
Si	63,00
No	37,00
<b>Total</b>	<b>100,00</b>

**Tabla No 2.4** Problemas de la red de datos  
**Elaboración:** Grupo Investigador

Gráfico No. 2.1



### Análisis

Se observa que del 100% de usuarios que utilizan la red de datos un 63% tienen diversas dificultades para acceder a su información, lo que quiere decir que este porcentaje de usuarios no están satisfechos de la seguridad que brinda actualmente un Router.

Tabla No 2.5

INFORMACION SEGURA	
Problemas con la red de Datos	Porcentaje (%)
Si	10,00
No	90,00
<b>Total</b>	<b>100,00</b>

Tabla No 2.5: información Segura

Elaboración: Grupo Investigador

Gráfico No 2.2

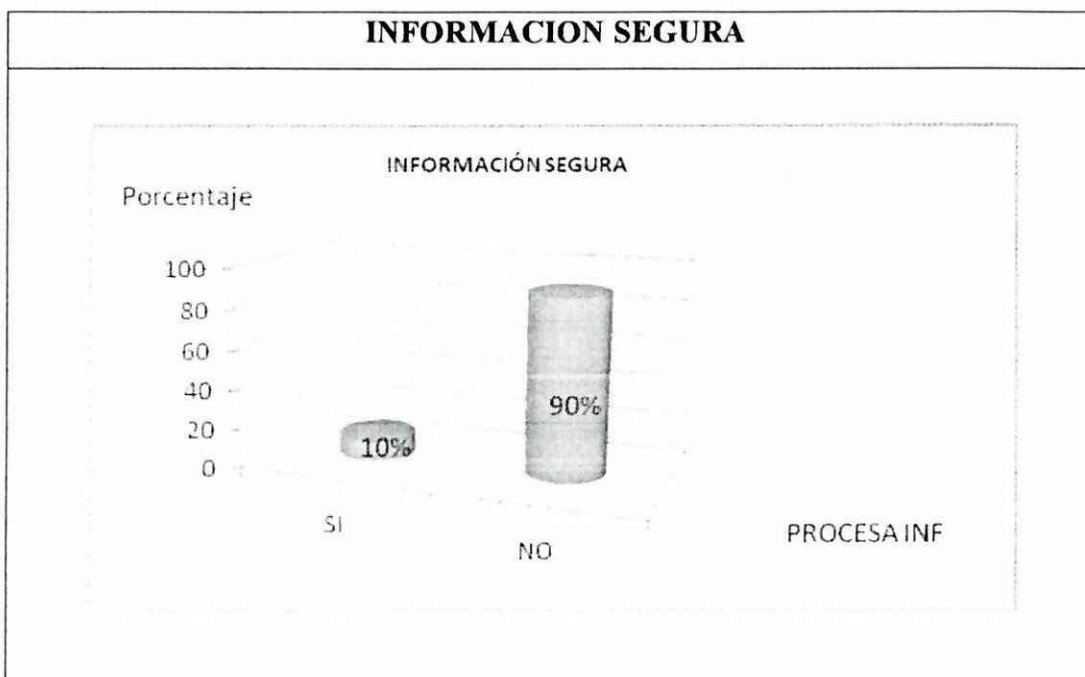


Gráfico No 2.2: Información Segura

Elaboración: Grupo Investigador

### Análisis

Se analiza que del 100%, de los usuarios, solo el 10% manifiesta que la infamación es rápida. Se puede deducir que la información que se procesa actualmente no es segura.

Tabla No 2.6

DISPOSITIVO DE SEGURIDAD	
Problemas con la red de Datos	Porcentaje (%)
Si	45,00
No	55,00
<b>Total</b>	<b>100,00</b>

Tabla No 2.6: Dispositivo de Seguridad

Elaboración: Grupo Investigador

Gráfico No 2.3



Gráfico No 2.3: Dispositivo de Seguridad

Elaboración: Grupo Investigador

### Análisis

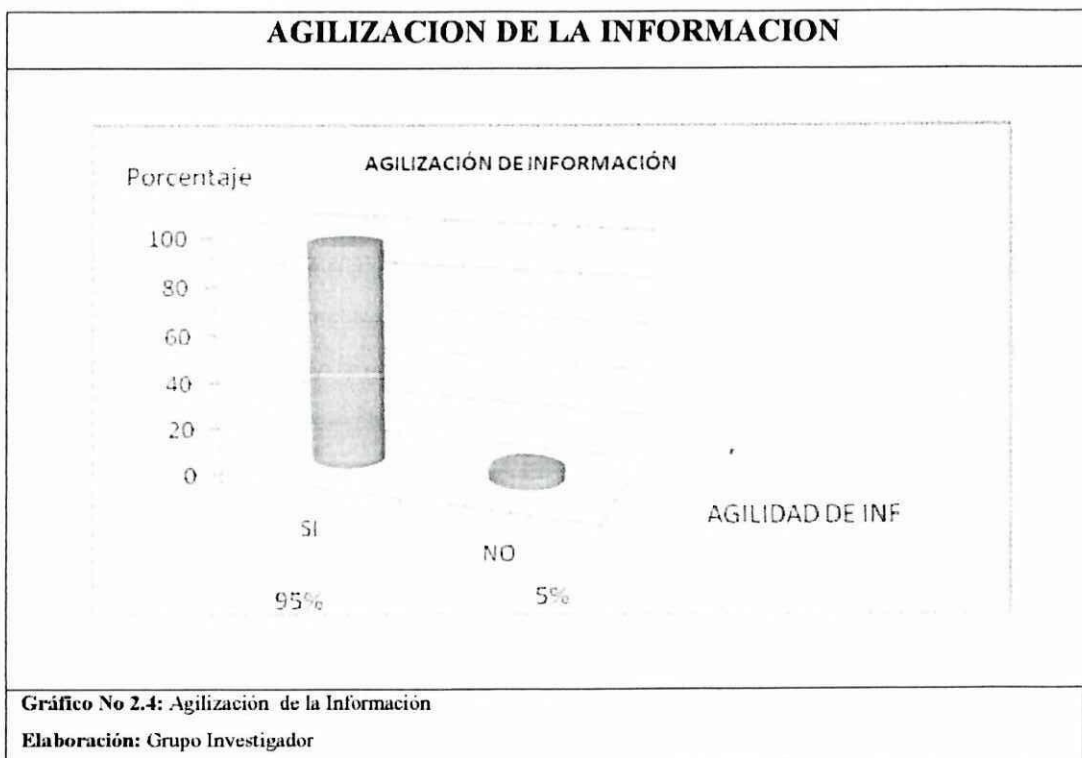
Se deduce que del 100% de usuarios que utilizan la red de datos, solo el 45% conocen que existe un dispositivo de seguridad en el CEYPSA.

Tabla No 2.7

AGILIZACION DE LA INFORMACION	
Problemas con la red de Datos	Porcentaje (%)
Si	95,00
No	5,00
<b>Total</b>	<b>100,00</b>

**Tabla No 2.7:** Agilización de la Información  
**Elaboración:** Grupo Investigador

Gráfico No 2.4



### Análisis

Se observa que del 100% de los usuarios, que utilizan la red de datos, el 95% piensa que un Router agilizaría el proceso de la información en el CEYPSA.

Tabla No 2.8

DESTINO DE INFORMACION	
Problemas con la red de Datos	Porcentaje (%)
Si	47,00
No	53,00
<b>Total</b>	<b>100,00</b>

Tabla No 2.8: Destino de la Información

Elaboración: Grupo Investigador

Gráfico 2.5

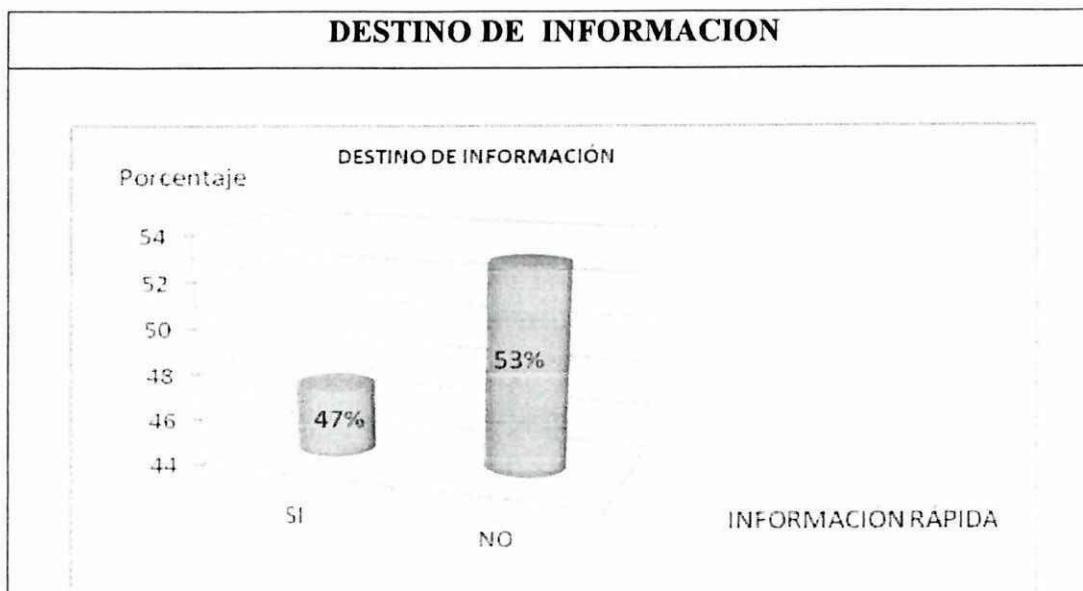


Gráfico 2.5: Destino de la Información

Elaboración: Grupo Investigador

### Análisis

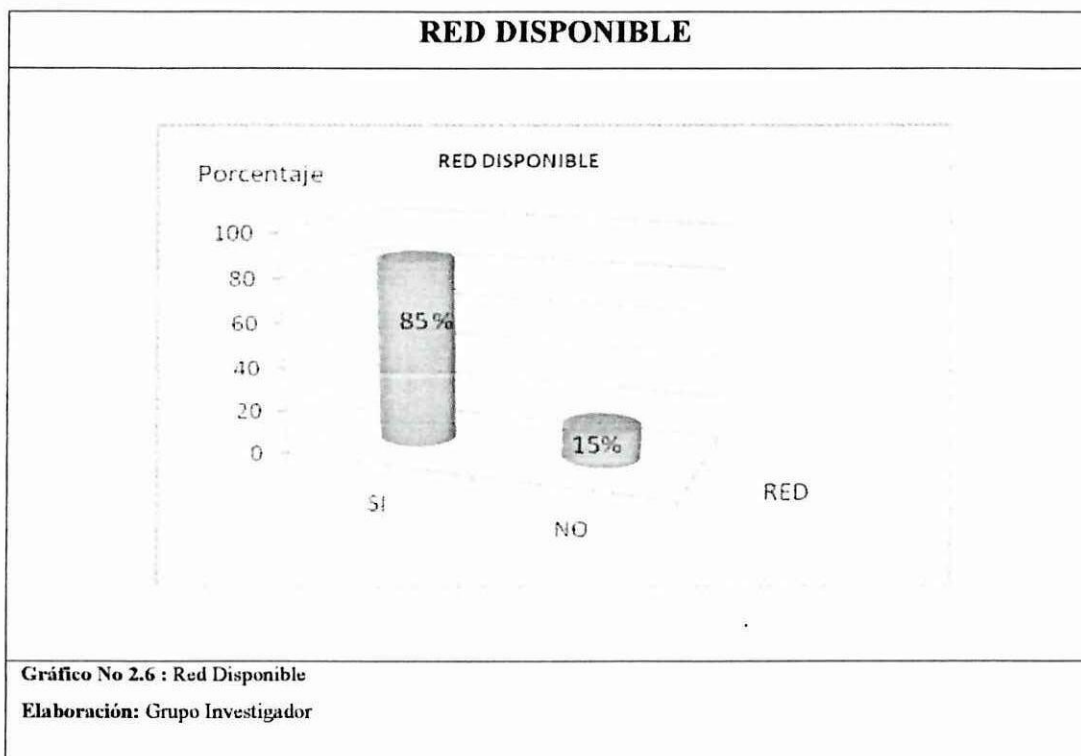
Se concluye que del 100% de usuarios que utilizan la red de datos, el 47% conoce que un Router permite que el destino de la información llegue en forma rápida y segura.

Tabla No 2.9

<b>RED DISPONIBLE</b>	
<b>Problemas con la red de Datos</b>	<b>Porcentaje (%)</b>
Si	85,00
No	15,00
<b>Total</b>	<b>100,00</b>

**Tabla No 2.9 : Red Disponible**  
**Elaboración:** Grupo Investigador

Gráfico No 2.6



### Análisis

Se deduce que del 100% de los usuarios que utilizan la red de datos, el 85% piensa que los departamentos existentes que se encuentran en red con un Router tendrían una red segura, rápida y eficiente.

Tabla No 2.10

<b>IMPORTANCIA DE UN ROUTER</b>	
<b>Problemas con la red de Datos</b>	<b>Porcentaje (%)</b>
Si	100,00
No	00,00
<b>Total</b>	<b>100,00</b>

Tabla No 2.10: Importancia de un Router

Elaboración: Grupo Investigador

Gráfico No 2.7

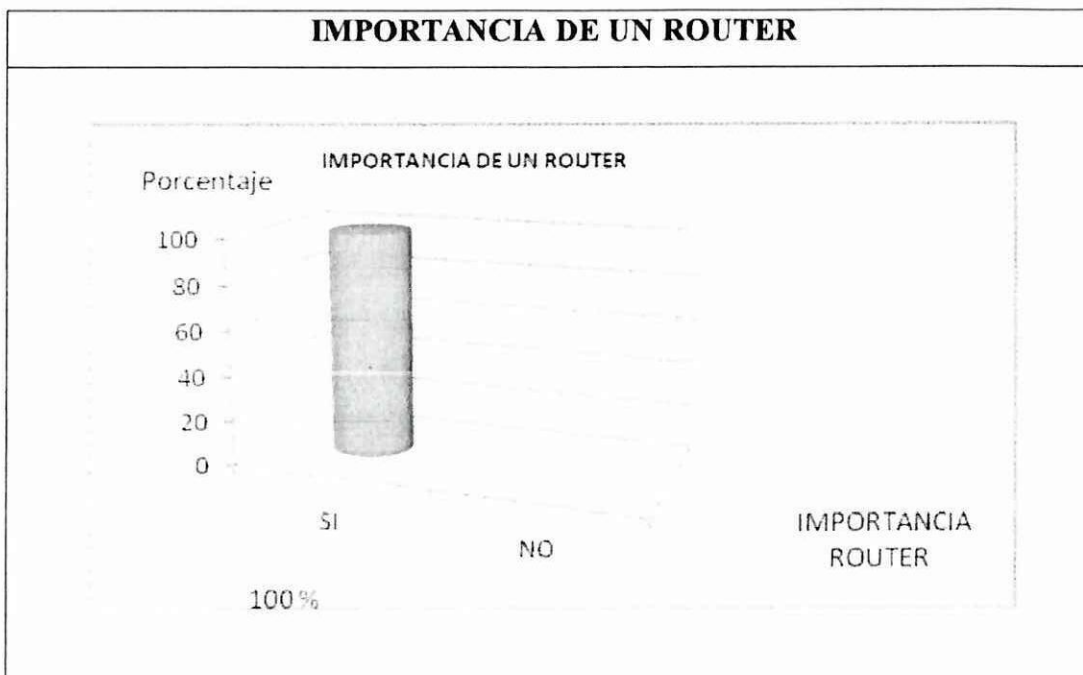


Gráfico No 2.7: Importancia de un Router

Elaboración: Grupo Investigador

### Análisis

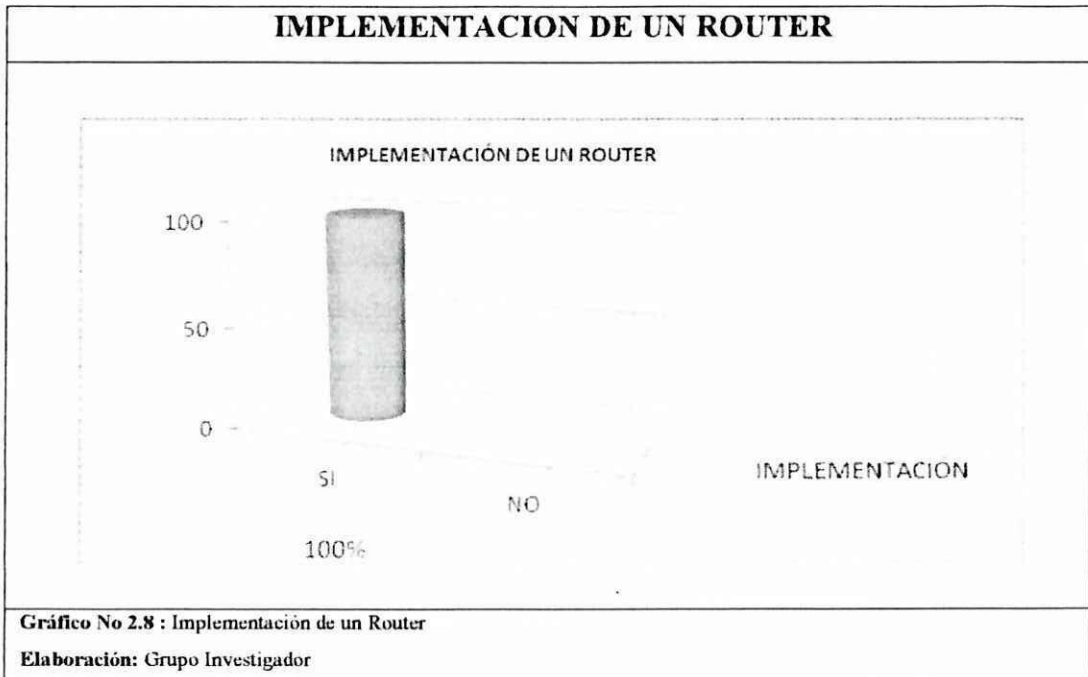
De los resultados obtenidos se deduce que los usuarios que utilizan la red de datos el 100%, piensa que es muy importante un Router, porque beneficia a que la información se procese en forma rápida y segura.

Tabla No 2.11

IMPLEMENTACION DE UN ROUTER	
Problemas con la red de Datos	Porcentaje (%)
Si	100,00
No	00,00
<b>Total</b>	<b>100,00</b>

**Tabla No 2.11 :** Implementación de un Router  
**Elaboración:** Grupo Investigador

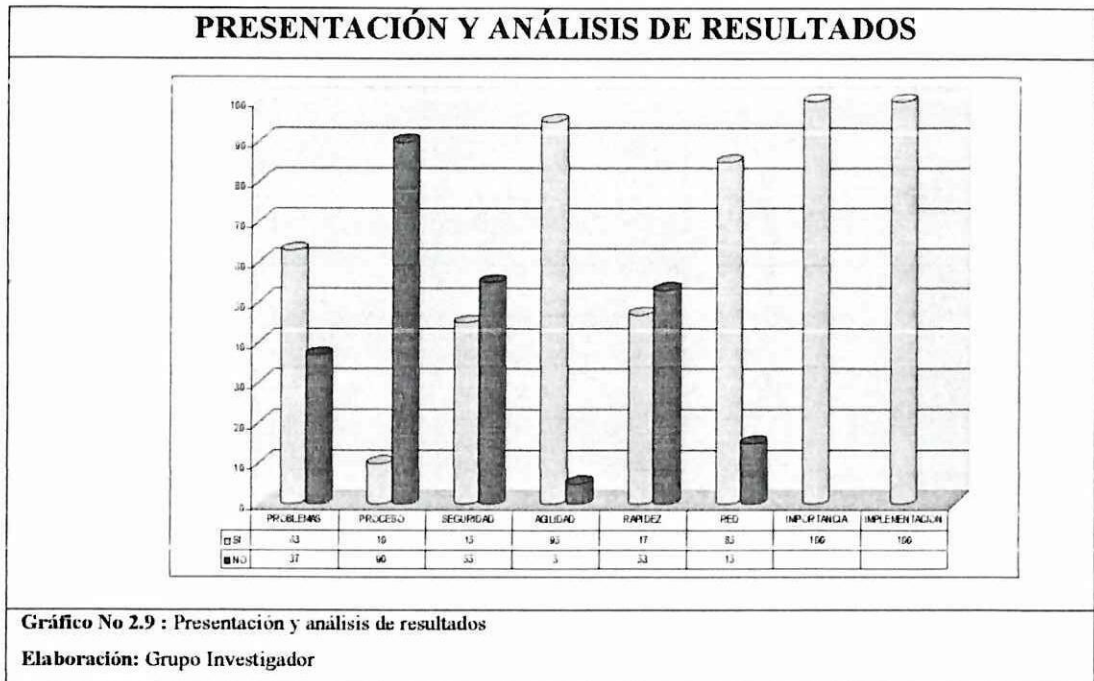
Gráfico No 2.8



### Análisis

Se puede notar que 100% de los usuarios que utilizan la red de datos, desean que se implemente un Router en el área de servicios informáticos del CEYPSA. Esto beneficiaría a toda el área que administra la red de datos y a los usuarios que utilizan la misma. Permitirá procesar la información en forma ágil, eficiente y rápida.

Gráfico No 2.9



## 2.5. Conclusiones

- El Departamento de Sistemas Informáticos del CEYPSA, no cuenta con un dispositivo de seguridad, esto dificulta a que los procesos se realicen en forma lenta e insegura debido a la falta de un Router.
- Se ha confirmado la inexistencia de un dispositivo que permita agilizar los servicios y proceso de la red de datos en el CEYPSA.
- Desconocimiento de los beneficios de un Router.
- La implementación de un Router permitirá procesar la información en forma eficiente y segura en la red de datos del CEYPSA.

## **2.6. Recomendaciones**

- Equipar al Departamento de Sistemas Informáticos del CEYPSA, con un Router, de esta forma el Administrador de la Red de Datos del CEYPSA (Ing. Adrian Mena) y los usuarios de las interfaces (Oficinas) podrá administrar en forma eficiente y rápida los servicios.
- Implementar el Router para mejorar la atención de los usuarios que utilizan la red de datos.
- Utilizar el manual de configuración, en caso de sufrir un daño en el software del Router CISCO.

## **2.7. Introducción a los requerimientos.**

Una investigación no puede ser exitoso sin una especificación correcta de los requerimientos, para ello se necesita muchas destrezas; un examen riguroso de las mismas permitirá obtener un buen resultado en la culminación de la investigación.

Para esto se llevo a cabo una investigación de la cual se determina una propuesta de los posibles requerimientos para la configuración de un Router en el servidor el cual permita optimizar la administración de la red de datos del Centro Experimental y Producción Salache (CEYPSA) de la Universidad Técnica de Cotopaxi.

Esta propuesta consiste en utilizar un Router CISCO que permita mejorar la red de datos, evitando cuello de botellas y optimizando las seguridades. Antes de acceder a la configuración se simulara en el software Simulador.

La técnica inmediata para identificar los requisitos del software se basa en los casos de uso, estos se capturan tanto los requisitos funcionales como los no funcionales que son específicos de cada caso de uso.

Los casos de uso nos ayudan a capturar los requerimientos del software. El administrador quiere que el software lleve a cabo ciertos casos de uso. Estos casos de uso capturan tanto los requerimientos funcionales como los no funcionales que son específicos de cada caso de uso.

### **2.7.1. Requerimientos**

Estos son una descripción de las necesidades o deseos de un producto, la meta primaria de la fase de inicio es identificar y documentar lo que en realidad se necesita en forma clara se lo comunique al cliente y a los miembros del equipo de desarrollo, el reto consiste en definirlos de modo que se detecten los riesgos y no se presenten sorpresas al momento de entregar el producto. Se recomienda los siguientes:

- Objetivo
- Usuarios.
- Metas.
- Funciones del Software.
- Elementos del Software.
- Funciones del Router.
- Elementos del Router.

Los requisitos adicionales son fundamentalmente requisitos no funcionales que no pueden asociarse a ningún caso de uso. Estos requisitos tienen un impacto en varios casos de uso o en ninguno.

Los requisitos adicionales se capturan de forma muy parecida a como se hacía en la especificación de requisitos tradicionales, es decir, como una lista de requisitos. Después se utilizan durante el análisis y el diseño junto al modelo de casos de uso.

### **2.7.2. Objetivo**

Este proyecto tiene por objeto configurar un Router para optimizar la administración de la red de datos del centro Experimental y Producción Salache (CEYPSA) de la Universidad Técnica de Cotopaxi

### **2.7.3. Usuarios**

- Dirección de Servicios Informáticos UTC
- Administrador Principal de la Red de Datos del CEYPSA
- Encargados de Laboratorios del CEYPSA
- Personal Directivo del CEYPSA
- Personal Administrativo del CEYPSA
- Departamento de Operaciones READYNET

### 2.7.4. Metas

El desarrollo de la investigación se centrará en optimizar todos los controles necesarios para un correcto uso de la información, es momento de cristalizar un proyecto ambicioso que se convertirá en una prioridad.

### 2.7.5. Funciones del Software

Las funciones a utilizarse en la administración del Router son dos:

- **Evidente.-** Debe realizarse, y el usuario debería saber que se ha realizado.
- **Oculto.-** Debe realizarse, aunque no es visible para los usuarios.

Tabla No 2.12

<b>FUNCIONES BÁSICAS DEL ROUTER</b>		
<b>No. Ref.</b>	<b>Función</b>	<b>Categoría</b>
R.1.1	Proveer método estándar de seguridad de la información.	Oculto
R.1.2	Proporcionar un control para administrar el Router	Evidente
R.1.3	Ofrecer un mecanismo de comunicación entre los procesos y el software	Oculto
R.1.4	Visualización grafica del control del Router	Evidente

Tabla No 2.12 : Funciones Basicas del Router  
Fuente: Grupo Investigador

### 2.7.6. Elementos del software

Los elementos del software son sus características o dimensiones. Los elementos del software pueden abarcar todas las funciones. Los elementos tienen un posible conjunto de detalles, los cuales tienden a ser valores discretos, confusos o simbólicos. Algunos elementos del software también pueden tener restricciones de frontera del atributo, que son condiciones obligatorias de frontera, generalmente en un rango numérico de los valores de un elemento.

Tabla No 2.13

<b>ATRIBUTOS DEL SISTEMA</b>	
<b>Elementos</b>	<b>Detalles y restricciones de frontera</b>
Tiempo de respuesta	(Restricción de frontera) tiempo real para la conexión del servidor y detectar el Router.
Metáfora de interfaz	(Detalle) maximiza una navegación fácil con teclado y mouse.
Tolerancia a fallas	(Restricción de frontera) debe prever que el Router se encuentre conectado correctamente.
Plataformas del sistema operativo	(Detalle)Windows.
<b>Tabla No 2.13</b> Atributos del Sistema <b>Fuente:</b> Grupo Investigador	

### 2.7.7. Funciones básicas del Router

Las siguientes funciones son las mínimas necesarias para el buen funcionamiento se plantea mediante dos categorías: Evidente, Oculta.

Tabla No 2. 14

<b>FUNCIONES BASICAS DEL ROUTER</b>		
<b>Ref. No.</b>	<b>Función</b>	<b>Categoría</b>
R1.1	Ofrecer un mecanismo entre el Router y el software.	Oculto
R1.2	Ofrecer un mecanismo de configuración del Router	Evidente
R1.3	Ofrecer seguridad y rapidez a la red de datos	Evidente
<b>Tabla No 2. 14</b> Funciones Básicas del Router <b>Fuente:</b> Grupo Investigador		

### 2.7.8. Elementos del Router

Tabla No 2. 15

<b>ELEMENTOS DEL ROUTER</b>	
<b>Descripción</b>	<b>Cantidad</b>
<b>Componentes Estructurales</b>	
Cable de consola azul (de RJ-45 a DB-9)	1
Adaptador de módem (de DB-9 a DB-25)	1
Cable de alimentación	1
Anclajes de montaje de bastidor de 19 pulgadas con tornillos	2
Anclaje de gestión de cables con un tornillo de montaje	1
Pies de goma para chasis para la aplicación de escritorio	1
<b>Tabla No 2. 15</b> Elementos del Router <b>Fuente:</b> Grupo Investigador	

## **2.8 Introducción a los Casos de Uso**

### **2.8.1 Casos de uso**

El conjunto de todos los Casos de Uso representa la totalidad de operaciones realizadas por el sistema. Una buena colección de Casos de Usos es fundamental para entender lo que los usuarios quieren. Son un punto de encuentro entre los usuarios y los profesionales de la informática.

Proporcionan un medio intuitivo y sistemático para capturar los requisitos funcionales con un énfasis especial en el valor añadido para cada usuario individual o para cada sistema externo. El caso de uso es un documento narrativo que describe la secuencia de eventos de un actor (agente externo) que utiliza un sistema para completar un proceso.

### **2.8.2. Actividades y dependencias**

Los casos de uso se toma en cuenta al personal encargado de las áreas de influencia por cuanto son ellos los que emplean y administran los recursos tecnológicos y operativos de los usuarios finales del CEYPSA-UTC los mismos que son:

- Dirección de Servicios Informáticos UTC.
- Administrador Principal de la Red de Datos CEYPSA.
- Administradores de áreas específicas (Oficinas y Laboratorios CEYPSA)

- Departamento de Operaciones READYNET

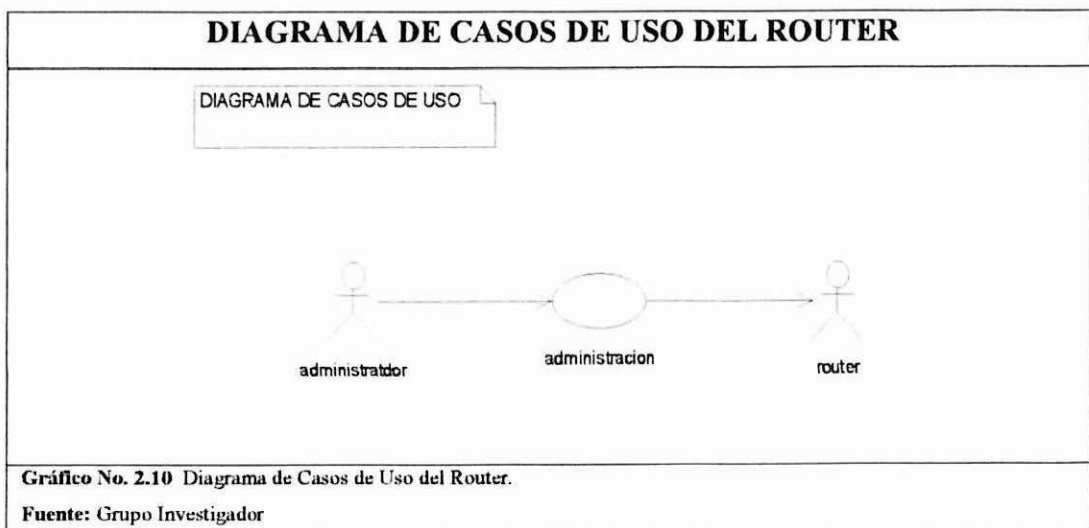
### 2.8.3. Actores

El actor es una entidad externa del sistema que de alguna manera participa en la historia del caso de uso. El modelo de casos de uso describe lo que hace el sistema para cada tipo de usuario.

### 2.8.4. Diagrama de los casos de uso

En la gráfica se muestra el diagrama de casos de uso del Router.

Gráfico No. 2.10



### **2.8.5. Descripción de procesos**

La descripción permite comprender de mejor manera los objetos o elementos que se constituirán en las piezas a desarrollarse en el sistema.

### **2.8.6. Casos de uso de alto nivel.**

Describen clara y concisamente el proceso que se quiere especificar. Los encabezados y la estructura de estos casos de uso son representativos. Sin embargo, El UML (Lenguaje Unificado de Modelado) no especifica un formato rígido; puede modificarse para atender las necesidades y ajustarse al espíritu de la documentación: ante todo, una comunicación clara.

Caso de uso	:	Administración.
Actores	:	Administrador, Router.
Tipo	:	Primario.
Descripción	:	El administrador se encarga de controlar el Router.

### **2.8.7 Casos de uso expandidos**

Es aquel que muestra más detalles que uno de alto nivel; este tipo de casos suele ser útiles para alcanzar un conocimiento más profundo de los procesos y de los requerimientos.

Caso de uso : Administración.

Actores : Administrador, Router.

Propósito : Administrar el Router

Resumen : El administrador se encarga de controlar los servicios, verificar las configuraciones del Router para facilitar a los usuarios una red de datos rápida, eficiente, segura y rápida

Tipo : Primario, Esencial

Referencias cruzadas: R1.1, R1.2, R1.3, R1.4.

Tabla No 2.16

<b>CURSO NORMAL DE LOS EVENTOS DE LA ADMINISTRACIÓN</b>	
<b>Acción del actor</b>	<b>Respuesta del Sistema</b>
	Proveer un método estándar para la seguridad de la información.
El administrador controla los servicios del Router	
	Ofrecer un mecanismo de comunicación entre los procesos y el software
	Visualización grafica del control del Router
<p><b>Tabla No 2.16:</b> Curso normal de los eventos de la Administración</p> <p><b>Fuente:</b> Grupo Investigador</p>	

## 2.9 Inicio de un ciclo de desarrollo

Este ciclo de desarrollo facilita la organización del trabajo y las iteraciones en cuatro fases fundamentales vea la (Tabla No. 2.17):

- **Inicio:** Visión aproximada, análisis del negocio, alcance, estimaciones imprecisas.
- **Elaboración:** Visión refinada, implementación iterativa del núcleo central de la arquitectura, resolución de los riesgos altos, identificación de más requisitos y alcance, estimaciones más relevantes.
- **Construcción:** Implementación iterativa del resto de requisitos del menor riesgo y elementos más fáciles, preparación para el despliegue.
- **Transición:** Pruebas beta, despliegue.

Tabla No. 2.17

CICLO DE DESARROLLO DEL PROYECTO				
DISCIPLINA	INICIO	ELABORACION	CONSTRUCCION	TRANSICION
REQUISITOS	▬			
DISEÑO		▬		
IMPLEMENTACION			▬	
PRUEBAS				▬
INTERACCIONES	#Iter.1	#Iter.1	#Iter.1	#Iter.1

Tabla No. 2.17: Ciclo de Desarrollo del Proyecto.  
Fuente: Grupo Investigador

## 2.10 Modelo conceptual de la Aplicación

Llamado modelo del dominio es una representación visual de las clases conceptuales u objetos del mundo real en un dominio de interés. El proceso Unificado define un modelo de dominio como uno de los artefactos que podrían crearse en la disciplina del Modelo del Negocio. El modelo del dominio se

representa con un conjunto de diagramas de clases en los que no se define ninguna operación. Pueden mostrarse:

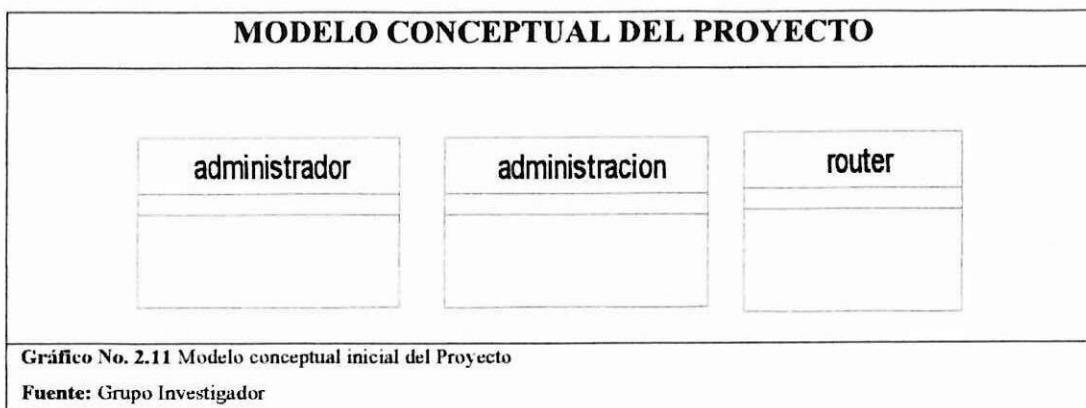
- Objetos del dominio o clases conceptuales
- Asociaciones entre las clases conceptuales.
- Atributos de las clases conceptuales.

Lista de conceptos adecuados para el control del Router:

- Administrador.
- Administración.
- Router.

La lista anterior de los nombres de conceptos puede representarse gráficamente.

Gráfico No. 2.11



### 2.10.1. Agregación de las asociaciones.

Es necesario identificar las asociaciones de los conceptos que se requieren para satisfacer los requerimientos de información de los casos de uso en cuestión, los que contribuyen a entender el modelo conceptual.

Gráfico No. 2.12

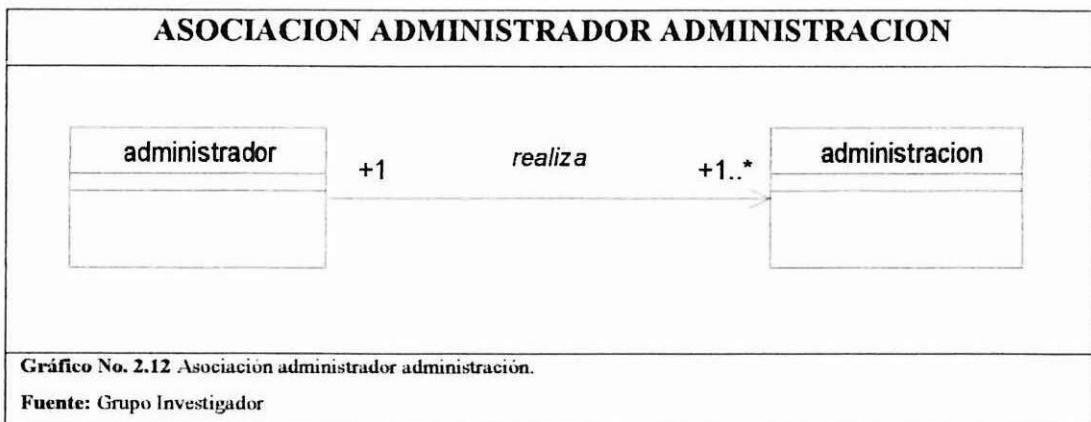


Gráfico No. 2.13

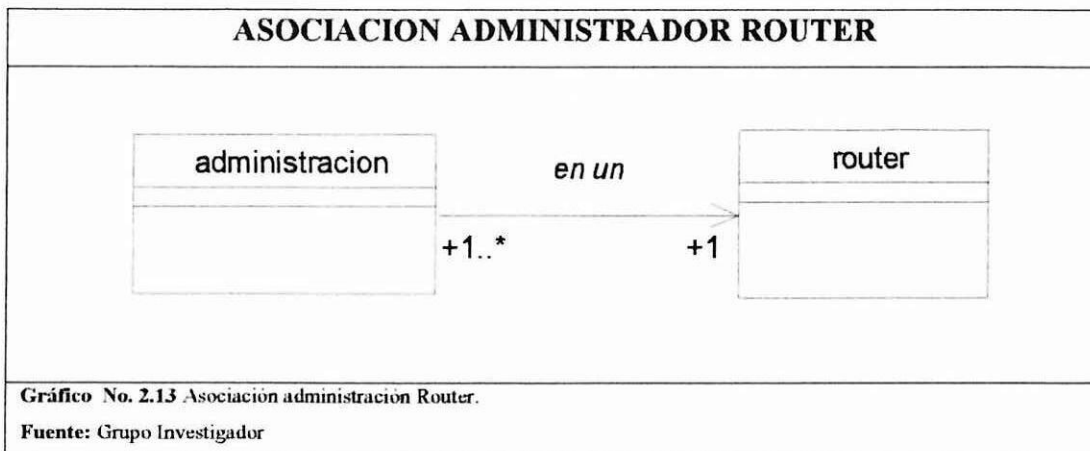


Gráfico No 2.14

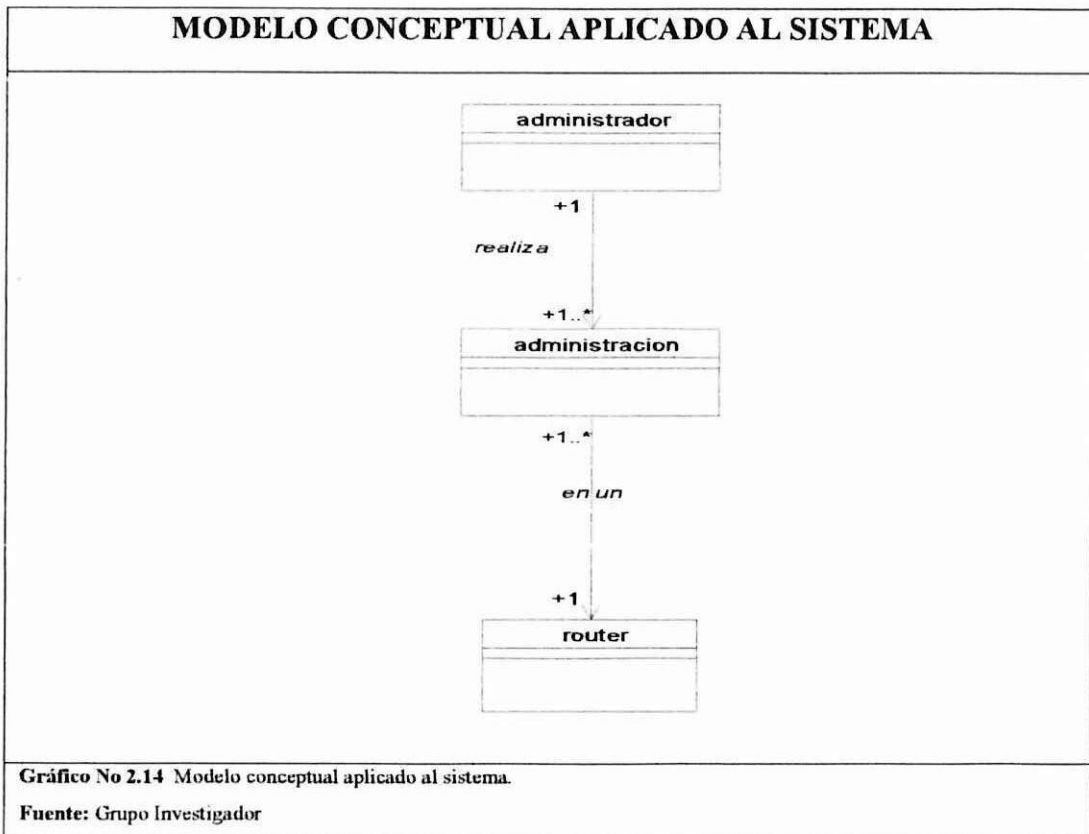


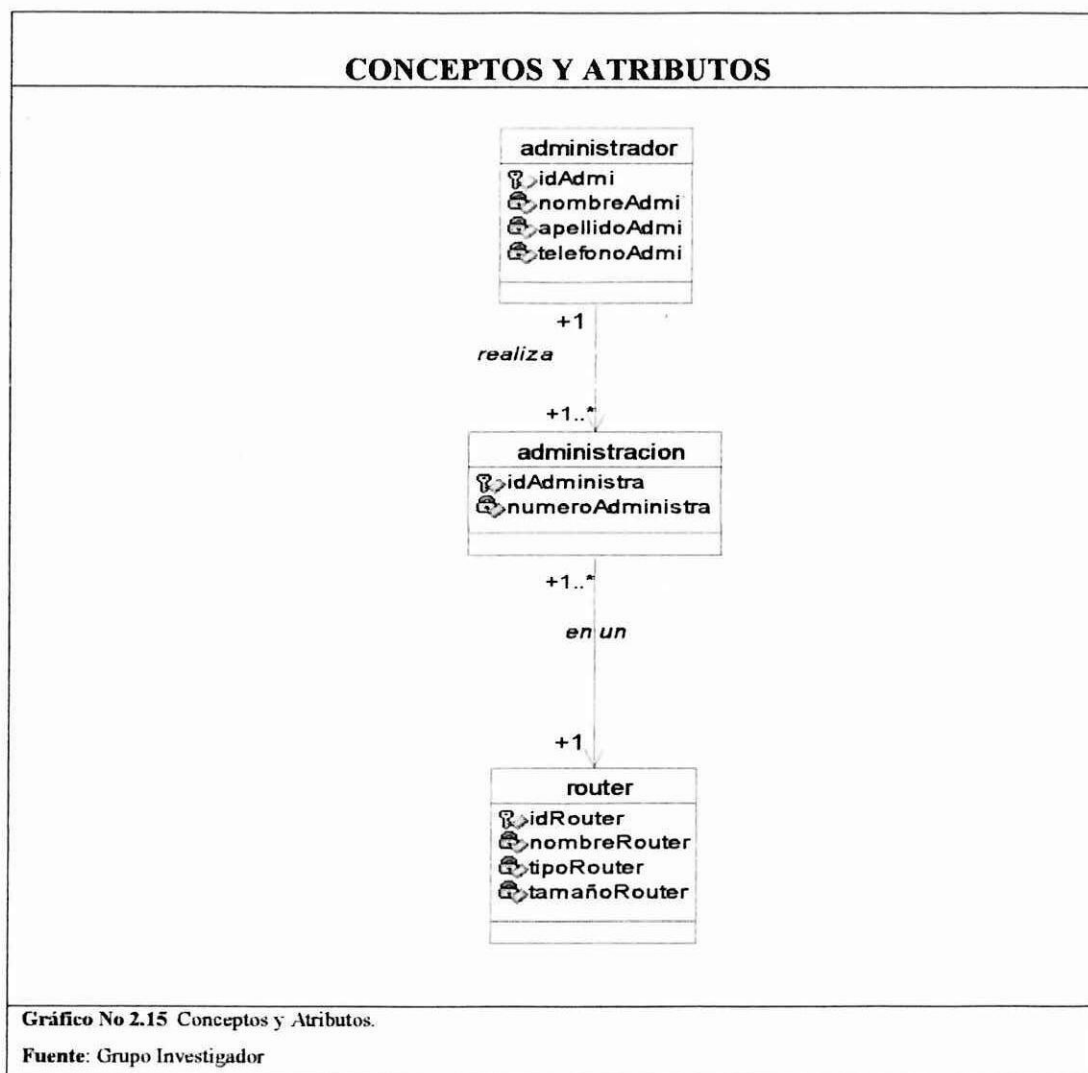
Gráfico No 2.14 Modelo conceptual aplicado al sistema.

Fuente: Grupo Investigador

### 2.10.2. Agregación de los atributos

Es necesario identificar los atributos de los conceptos que se necesitan para satisfacer los requerimientos de información de los casos de uso.

Gráfico No 2.15



## 2.11. Diccionario de datos

Se definen todos los términos que requieren explicarse para mejorar la comunicación y menorar el riesgo de malos entendidos.

Tabla No 2.18

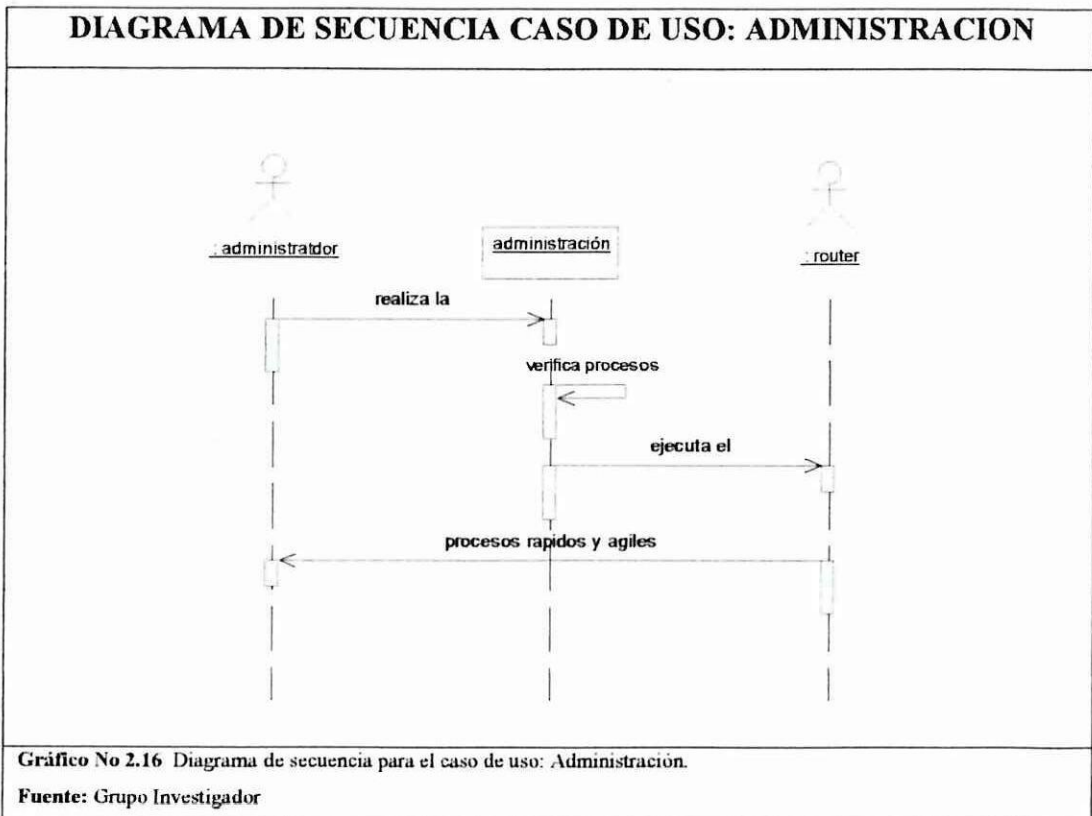
<b>GLOSARIO DE TERMINOS</b>		
<b>Término</b>	<b>Categoría</b>	<b>Observaciones</b>
Administración	Caso de uso	Control del Router
Administrador	Tipo	Responsable en administrar el control del Router
idAdmi	Atributo	Clave del administrador
nombreAdmi	Atributo	Nombre del administrador
apellidoAdmi	Atributo	Apellido del administrador
telefonoAdmi	Atributo	Teléfono del administrador
Administración	Tipo	Control del Router
idAdministra	Atributo	Clave para la administración
numeroAdministra	Atributo	Numero de acciones para administrar
Router	Tipo	Dispositivo de protección de seguridad
nombreRouter	Atributo	Nombre del Router
tipoRouter	Atributo	Tipo del Router
tamañoRouter	Atributo	Tamaño del Router
<p><b>Tabla No 2.18</b> Glosario de Términos  <b>Fuente:</b> Grupo Investigador</p>		

## 2.12. Diagramas de secuencia del sistema.

Un diagrama de Secuencia muestra una interacción ordenada según la secuencia temporal de eventos. En particular, muestra los objetos participantes en la interacción y los mensajes que intercambian ordenados según su secuencia en el tiempo. El eje vertical representa el tiempo, y en el eje horizontal se colocan los objetos y actores participantes en la interacción, sin un orden prefijado. Cada objeto o actor tiene una línea vertical, y los mensajes se representan mediante flechas entre los distintos objetos. El tiempo fluye de arriba abajo. Se pueden

colocar etiquetas (como restricciones de tiempo, descripciones de acciones, etc.) bien en el margen izquierdo o bien junto a las transiciones o activaciones a las que se refieren.

Gráfico No 2.16



### 2.13 Análisis e interpretación operativa de resultados

Para el cálculo del Análisis e interpretación operativa de resultados se tomo en cuenta a los encargados de las áreas designadas por la Red de datos del CEYPSA, por cuanto son ellos los que administran los recursos tecnológicos y operativos de los usuarios finales del CEYPSA-UTC, con lo que basados en los indicadores se pudo detectar que se tubo todo a favor como.

- Los recursos tecnológicos en hardware y software que posee el CEYPSA superan ampliamente los requisitos estandarizados para el óptimo desarrollo de la Configuración del Router CISCO 2811 para optimizar la Administración de la Red de Datos del CEYPSA.
- Se dominó considerablemente los diagnósticos de la funcionalidad del Router
- El Impacto de la Configuración Router en la administración de la red de datos del CEYPSA mejora disponibilidad de la Red de acuerdo a los siguientes parámetros:
  - Metáfora de interfaz : Maximiza una navegación fácil con teclado y mouse.
  - Plataformas : Sistema operativo Windows XP
  - Tiempo de respuesta : Tiempo real para la conexión del servidor y detectar el Router.
  - Tolerancia a fallas : Debe prever que el Router se encuentre conectado correctamente.
- La técnica utilizada para identificar los requisitos del software se basó en los Casos de Uso (UML), estos capturaron tanto los requisitos funcionales como los no funcionales así como los requerimientos del hardware.
- Se cumplió dilatadamente con los requerimientos de los administradores y usuarios de la Red de Datos del CEYPSA. En cuanto a la conformidad y cobertura de las necesidades o deseos del Router, en la fase de inicio se ha identificado y documentado los requisitos de usuario que en realidad se utilizó, satisfaciendo de forma clara las expectativas del Administrador con los siguientes parámetros:
  - Ostentan un método estándar para la seguridad de la información
  - Poseen control para administrar el Router
  - Mantienen un mecanismo de comunicación entre los procesos y el software
  - Gozan de visualización grafica del control del Router

## 2.14 Verificación de la Hipótesis

Una vez contabilizados los datos de las encuestas aplicadas al personal usuario de la Red de Datos del CEYPSA se puede observar en detalle el resultado de estas como se detalla a continuación:

1. El 63% de los encuestados concuerdan en que tienen dificultades para acceder a la información de la Red.
2. El 10% de los usuarios encuestados manifiestan que la información es segura.
3. El 45% de los usuarios manifiestan que si conocen de la existencia de un dispositivo de seguridad en el CEYPSA.
4. El 95% de los usuarios encuestados manifiestan que un Router agilizará y optimizará los procesos de información en la Red de Datos del CEYPSA.
5. El 47% de usuarios tienen conocimiento de que un Router permite información llegue a su destino de una manera rápida y segura.
6. El 85% de los usuarios confían que los departamentos enlazados en red con un Router tendrían una administración segura, rápida y eficiente.
7. El 100% de usuarios encuestados manifiestan que es muy importante implementar Router, en las Redes de Datos.
8. El 100% de usuarios red de datos encuestados, desean que se implemente un Router en el área de servicios informáticos del CEYPSA.

En conclusión los usuarios encuestados manifiestan que la implementación de un Router permitirá administrar la Red en forma eficiente y segura para mejorar la atención de los usuarios que utilizan la Red de Datos CEYPSA.

Basados en uno de los Objetivos de la Dirección de Servicios Informáticos de la Universidad Técnica de Cotopaxi como es el de: Elevar el nivel de formación del personal docente y administrativo, así como de los estudiantes en el uso de las Nuevas Tecnologías de la Información y la Comunicación. El Grupo investigador

ha desarrollado una investigación exitosa basado en las directrices dadas por la propia compañía Cisco sobre Seguridad de la información.

Para ello se necesita muchas destrezas técnicas; por lo que el desarrollo del presente trabajo se basa en dos aspectos de mucha importancia como son:

- La utilización de los sistemas de configuración del propio Router (interfaz Exec), que es el sistema operativo propiamente dicho.
- La utilización del SDM que permite la configuración en modo gráfico del equipo.

Tras el estudio realizado, la elaboración y las respuestas a las encuestas, y lo extraído de las fuentes bibliográficas, se puede hacer una verificación de las hipótesis. Donde hay que aclarar que, desde nuestro punto de vista no estábamos muy lejos de la realidad. Debemos decir que según los datos obtenidos, podemos afirmar que la hipótesis fue verdadera en virtud de que si fue factible la Configuración de un Router cumpliendo cada uno de los requerimientos establecidos por los encargados de la Administración de la Red de Datos del Centro Experimental y Producción Salache (CEYPSA) de la Universidad Técnica de Cotopaxi y con los estándares establecidos para una eficaz seguridad en las redes informáticas.

# CAPITULO III

## LA PROPUESTA

### 3.1 Modelo de Análisis y Diseño

Durante este paso se logra una solución lógica que se funda en el paradigma orientado a objetos. Su esencia es la elaboración de diagramas de interacción, que muestran gráficamente cómo los objetos se comunicarán entre ellos a fin de cumplir con los requerimientos.

En la fase de análisis del desarrollo se da prioridad al conocimiento de los requerimientos, los conceptos y las operaciones relacionadas con el sistema. A menudo la investigación y el análisis se caracterizan por centrarse en cuestiones concernientes al qué: cuáles son los procesos, los conceptos, etc. En el UML hay otros artefactos que sirven para capturar los resultados de una investigación; a continuación se describe un grupo mínimo de ellos que fueron plasmados en la etapa anterior.

Caso de uso	:	Administración.
Actores	:	Administrador, Router.
Tipo	:	Primario.
Descripción	:	El administrador se encarga de controlar el Router.

Gráfico No.3.1

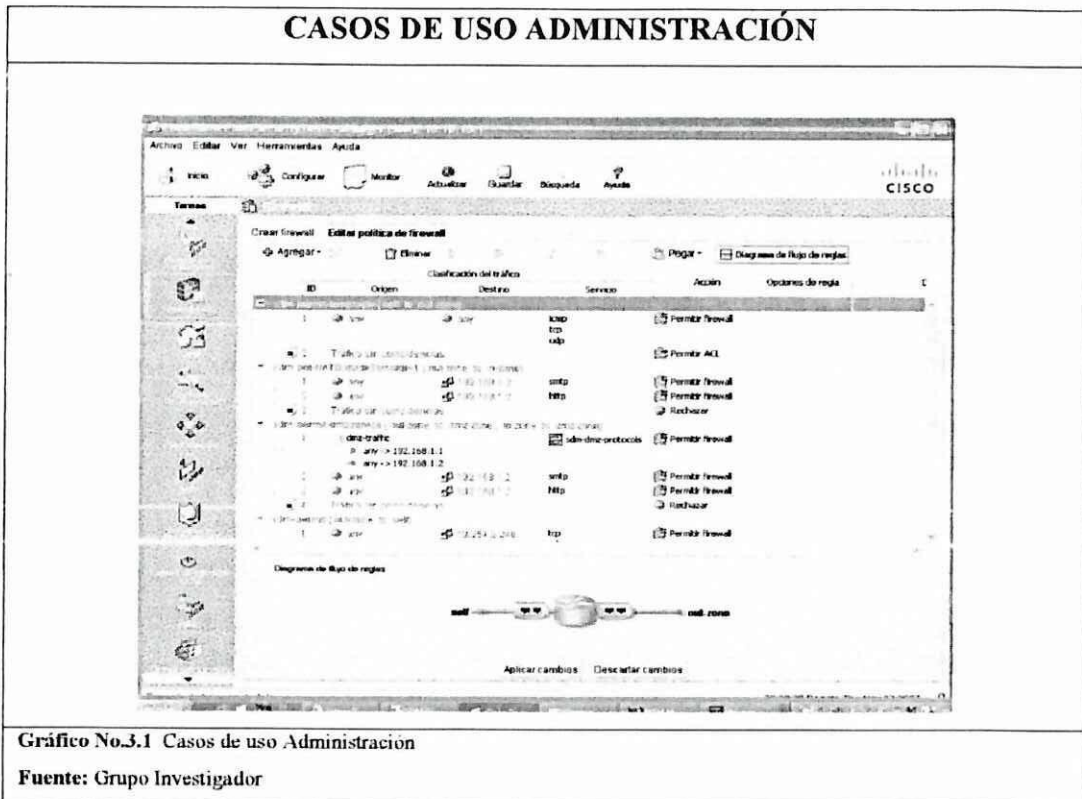


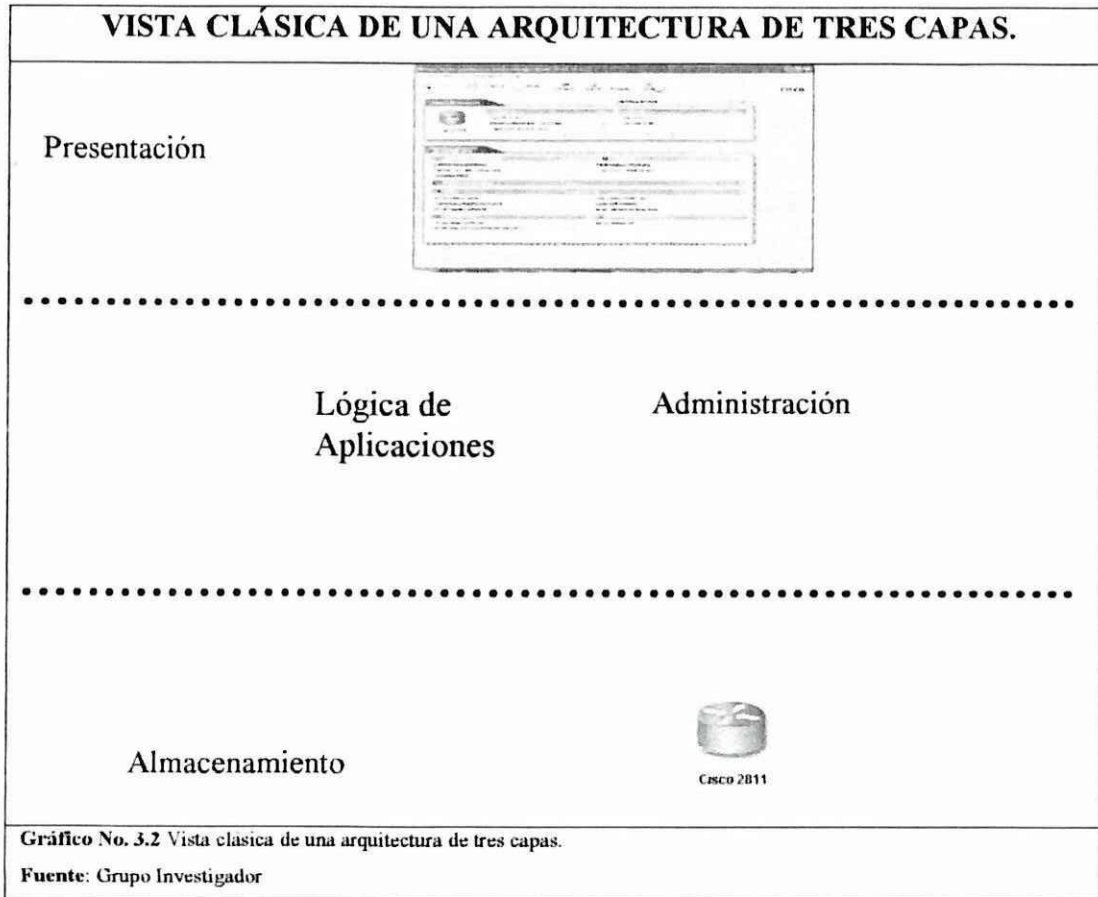
Gráfico No.3.1 Casos de uso Administración  
Fuente: Grupo Investigador

### 3.2. Algunos aspectos del diseño del sistema.

En sistema de información abarca una interfaz para el usuario y el almacenamiento persistente de datos se conoce con el nombre de arquitectura de tres capas. He aquí una descripción clásica de las tres capas verticales:

1. Presentación: ventanas, reportes, etcétera.
2. Lógica de aplicaciones: tareas y reglas que rigen el proceso.
3. Almacenamiento: mecanismo de almacenamiento persistente.

Gráfico No. 3.2



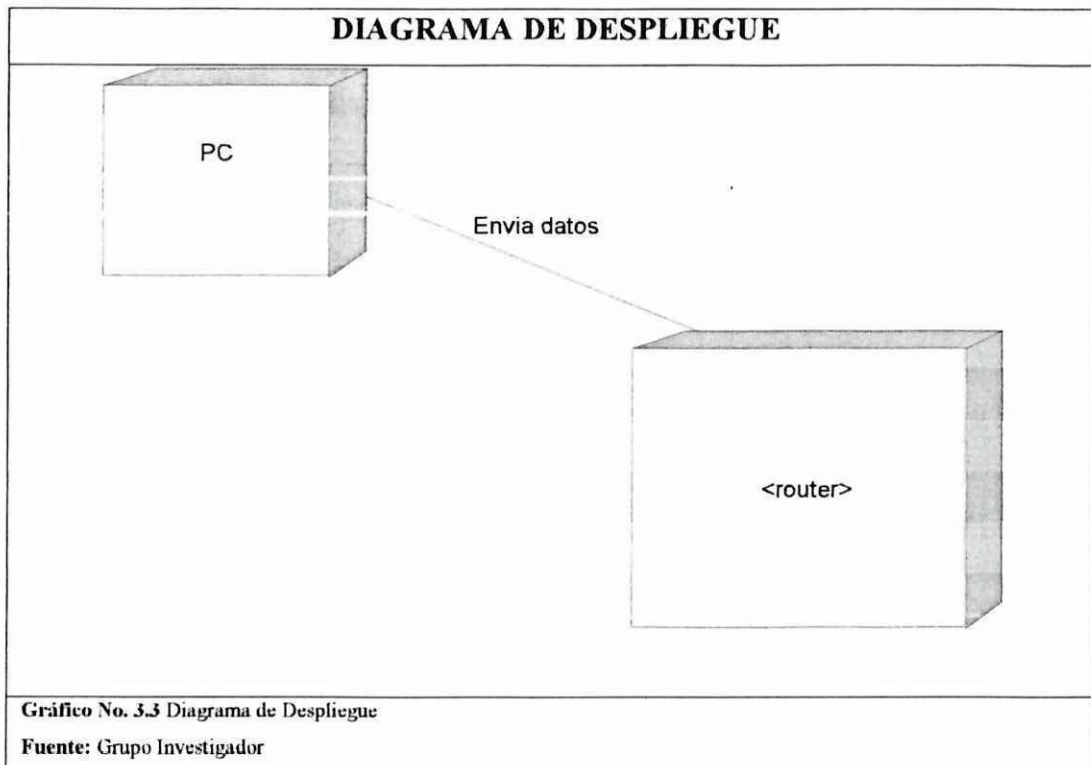
### 3.3 Mapeo de los diseños para codificación.

Una vez concluidos los diagramas de clases del diseño y destinados al ciclo de desarrollo actual en la aplicación, dispondremos de suficientes detalles para generar un código que utilizaremos en la capa del dominio de los objetos.

Si se quiere reducir el riesgo y aumentar la probabilidad de conseguir una aplicación adecuada, el desarrollo debería basarse en un suficiente modelado del análisis y diseño antes de iniciar la codificación. Ello no significa que durante la

programación no tengan cabida los prototipos ni el diseño: las modernas herramientas del desarrollo ofrecen un excelente ambiente par examinar rápidamente métodos alternos, y normalmente vale la pena dedicar poco o mucho tiempo al diseño por la codificación.

Gráfico No. 3.3



## 3.4. Implementación y pruebas

### 3.4.1 Introducción

Este documento es una Especificación de Requisitos Software (ERS) para el Router CISCO 2811 del Centro de Experimentación Salache de la Universidad Técnica de Cotopaxi, se constituye en el medio oficial de proveer documentación

técnica a los usuarios del Router CISCO 2811 del CEYPSA; y resalta sus características más significativas. También describe las instrucciones de diseño que permiten determinar los requisitos específicos.

Desafortunadamente, las intrusiones en redes por parte de usuarios externos e internos se han convertido en un suceso habitual, lo que significa que las organizaciones deben instalar alguna protección contra las mismas. Un Router CISCO representa generosos recursos económicos y no supone un impedimento para el normal flujo de tráfico. Por lo tanto, debe asegurarse de que el Router CISCO esté configurado para ser tan rentable y eficaz como sea posible.

### **3.4.2 Contenido**

Este módulo contiene información, instrucciones así como los procedimientos pertinentes a todos los trabajos de operación mantenimiento y modificación de configuraciones del Router CISCO 2811 del CEYPSA. Todo su contenido ha sido elaborado teniendo en cuenta las necesidades observadas en la Red de Datos del CEYPSA. La información precisada en este Manual de Usuario se halla establecida en función de varios programas de muestreo aplicados por el grupo postulante, basados en publicaciones emitidas por la Compañía CISCO Systems así como en varias organizaciones gubernamentales y privadas que basan el flujo de sus Redes en Routers CISCO.

### **3.4.3 Usuarios del Router CISCO 2811**

Los usuarios autorizados por la Dirección de Servicios Informáticos de la Universidad Técnica de Cotopaxi y a los proveedores de del Servicio de Internet

siendo en este caso la empresa READYNET. Este documento será el canal de comunicación entre las partes implicadas, tomando parte en su confección miembros de cada parte.

### **3.4.4 Uso del módulo**

Antes de comenzar a dar uso operativo a este módulo, el lector debería poseer algunos conocimientos generales sobre las instrucciones de los Routers CISCO. También resulta útil ponerse al corriente a cerca del origen, uso, aplicación y cambios de las instrucciones de diseño que se presentan en este módulo, teniendo en cuenta consideraciones importantes como el crecimiento de la red y el cambio de configuraciones en el Router. Este módulo define también las distintas clases de instrucciones de rediseño, el responsable de manipular estos cambios debe poder seleccionar la clase que se ajuste mejor a sus necesidades. A partir de los conocimientos y la terminología técnica proporcionados en este módulo, podrá analizar con los usuarios del Router CISCO los cambios que pueden ofrecerle y evaluar si se adecúan o no a sus necesidades.

### **3.4.5 Visión general del documento**

Más allá de la experiencia o conocimientos que cada uno de nosotros tenga en la administración y configuración Redes Informáticas, al momento de tener que realizar o modificar la configuración de una interfaz, es importante que tengamos en cuenta algunas claves, que son comunes a todas las interfaces de los dispositivos CISCO. Ante todo, todos los comandos relacionados con la configuración de algún aspecto de las interfaces, se ejecutan en el modo configuración de consola.

Con el fin de conocer las principales funciones que realiza un Router , así como los datos asociados, los factores, restricciones, supuestos y dependencias que afectan al desarrollo de la Configuración del Router CISCO 2811 del CEYPSA, se ha clasificado de la siguiente manera:

## **3.5 Generalidades de los Router CISCO**

### **3.5.1 Introducción**

CISCO SYSTEMS es una compañía californiana dedicada a las redes, en sus catálogos se incluyen Router s, Switches, Cortafuegos, etc. CISCO vende tanto el Hardware como Software incluyendo varias versiones de IOS (Sistemas Operativos) por lo que el 70% del tráfico de Internet circula por dispositivos CISCO

Una investigación no puede ser exitosa sin una serie de pruebas operativas con parámetros que cumplan con los requerimientos, para ello se necesita muchas destrezas técnicas; por lo que el desarrollo del presente trabajo se basa en dos aspectos de mucha importancia:

- La utilización de los sistemas de configuración del propio Router (interfaz Exec), que es el sistema operativo propiamente dicho
- SDM que permite la configuración en modo gráfico del equipo.

## 3.5.2 Principios de un Router

### 3.5.2.1 La familia Sistemas Operativos (IOS)

Hay muchas versiones de Sistemas Operativos (IOS) cuya nomenclatura está estandarizada

- **Mainline:** Versión de IOS más estable. No se añaden funcionalidades sobre y sólo se realizan actualizaciones por bugs
- **T: Technology.** Modifica una mainlinea por una demanda de una actualización por bug o una nueva funcionalidad. El hardware no está incluido.
- **S: Service Provider.** Optimizada para los clientes proveedores de Servicios.
- **SB: Funcionalidad** Funcionalidad y hardware de banda ancha de equipos de gama media para el borde de red (Router s)
- **SX:** Equipos Ethernet-LAN de altas prestaciones para core de red (switchs)
- **SE, SG:** Equipos Ethernet-LAN de rango medio-bajo (switchs)
- **SR:** Equipos Ethernet-LAN de altas prestaciones para borde de red (Routers)
- **E: Enterprise.** Optimizada para entornos empresariales.
- **B: Broadband.** Optimizada para banda ancha
- **XR:** Optimizada para el Core de red y con capacidad de direccionar terabits de tráfico.

### 3.5.2.2 Numeración T

La versión principal actual del Sistema Operativo (IOS) para el Router CISCO 2811 del CEYPSA es la 12.

- **12.4(7a)** Es una versión mainline 12.4 release 7a
- **12.4(9)T3** Es la tercera versión T basada en la mainline 12.4(9)

### 3.5.2.3 Numeración S

- **12.2(28)SB1**: Primera revisión de la 12.2(28) de SB (para Routers medianos)

### 3.5.2.4 Numeración XR:

- No tiene más que números: 12.3.1

## 3.5.3 Partes de un Router

Esta sección contiene un Repertorio total de todos los componentes Aplicables del Router CISCO 2811, entre estos tenemos:

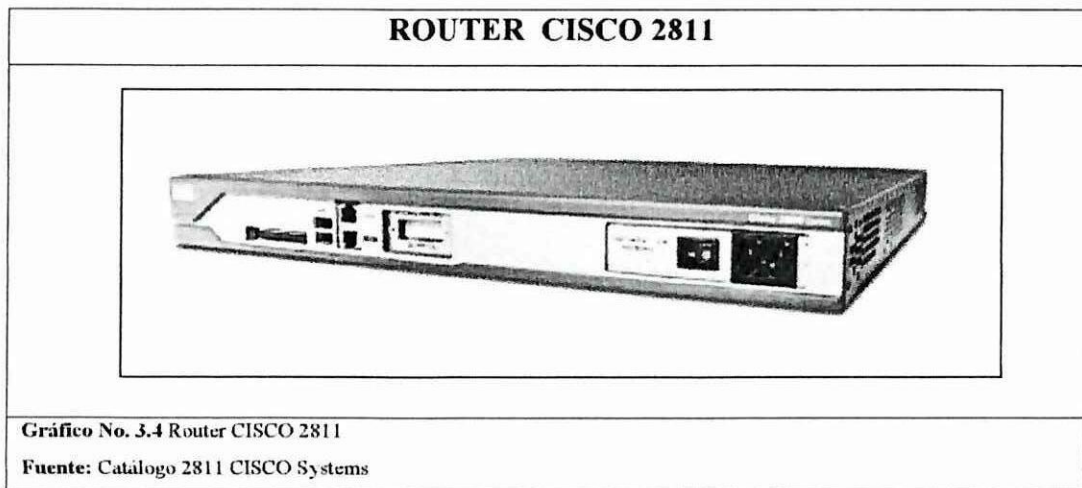
- **RAM/DRAM** : Guarda tablas de enrutamiento, ARP, valores temporales.
- **NVRAM** : Almacena la configuración
- **FLASH** : Almacena el IOS arrancable
- **ROM** : Guarda el bootstrap.
- **INTERFACE** : Conexiones de red

### 3.5.4 Actualizaciones de un Router

- **FCS** : First Customer Shipment. A disposición del cliente
- **EoS** : End of Sale. Se deja de vender el producto, pero se siguen sacando actualizaciones.
- **EoE** : End of Engineering. No se sacan más actualizaciones pero se sigue dando soporte.
- **EoL** : End of Life. Únicamente se da soporte en caso de migración a una versión más actual.

### 3.6 Router CISCO 2811

Gráfico No. 3.4



### 3.6.1 Especificaciones de un Router CISCO Serie 2811

Tabla 3.1

<b>CARACTERISTICAS DEL ROUTER CISCO 2811</b>	
<b>GENERAL</b>	
Tipo de dispositivo	Encaminador
Factor de forma	Externo - modular - 1U
Anchura	43.8 cm
Profundidad	41.7 cm
Altura	4.5 cm
Peso	6.4 kg
<b>MEMORIA</b>	
Memoria RAM	256 MB (instalados) / 760 MB (máx.)
Memoria Flash	64 MB (instalados) / 256 MB (máx.)
<b>CONEXIÓN DE REDES</b>	
Tecnología de conectividad	Cableado
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Red / Protocolo de transporte	IPSec
Protocolo de gestión remota	SNMP 3
Indicadores de estado	Actividad de enlace, alimentación
Características	Protección firewall, cifrado del hardware, alimentación mediante Ethernet (PoE), VPN, soporte de MPLS, filtrado de URL
Cumplimiento de normas	IEEE 802.3af
<b>EXPANSION / CONECTIVIDAD</b>	
Total ranuras de expansión (libres)	4 ( 4 ) x HWIC   2 ( 2 ) x AIM   1 ( 1 ) x NME   2 ( 2 ) x PVDM   2 memoria   1 Tarjeta CompactFlash
Interfaces	6 x red - Ethernet 10Base-T/100Base-TX - RJ-45   2 x USB   1 x gestión -

	consola   1 x red – aux
<b>ALIMENTACION</b>	
Dispositivo de alimentación	Fuente de alimentación – interna
Voltaje necesario	CA 120/230 V ( 47 - 63 Hz )
<b>SOFTWARE</b>	
OS proporcionado	CISCO IOS 12.3(8)T
Sistema operativo requerido	Microsoft Windows 98 Second Edition
<b>PARAMETROS DE ENTORNO</b>	
Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	40 °C
Ámbito de humedad de funcionamiento	5 - 95%
<b>Tabla No. 3.1</b> Características Router CISCO 2811	
Fuente: Catálogo 2811 CISCO Systems	

### 3.6.2 Conectividad del Router Cisco 2811 del CEYPSA

Gráfico No. 3.5

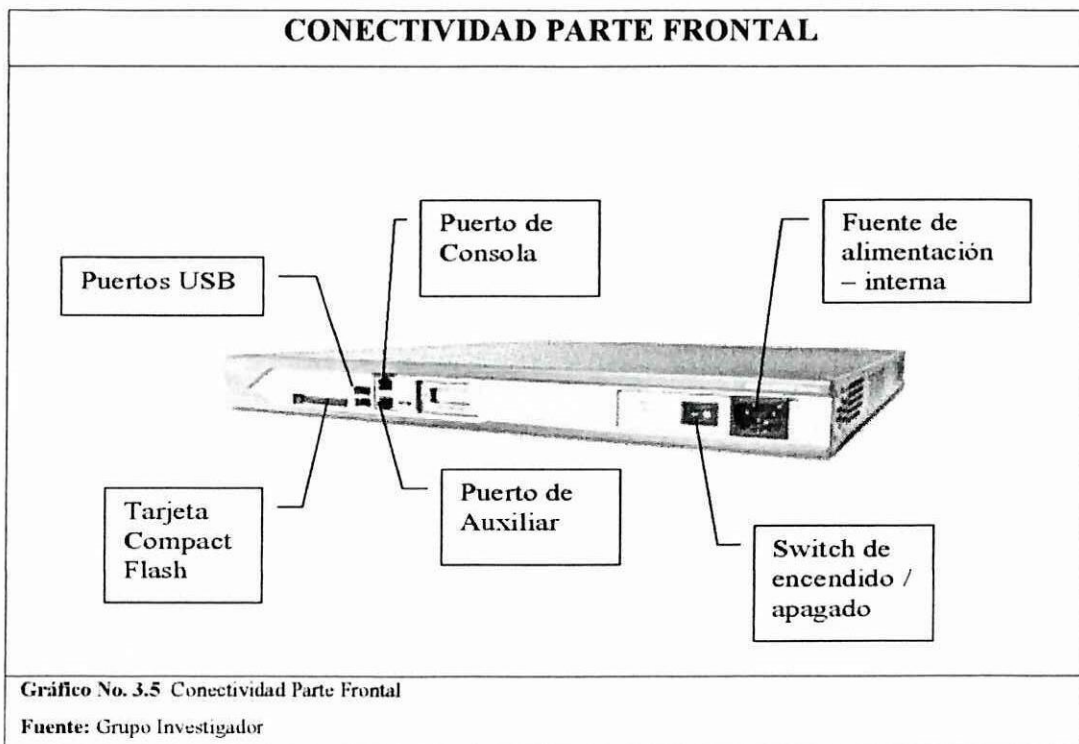
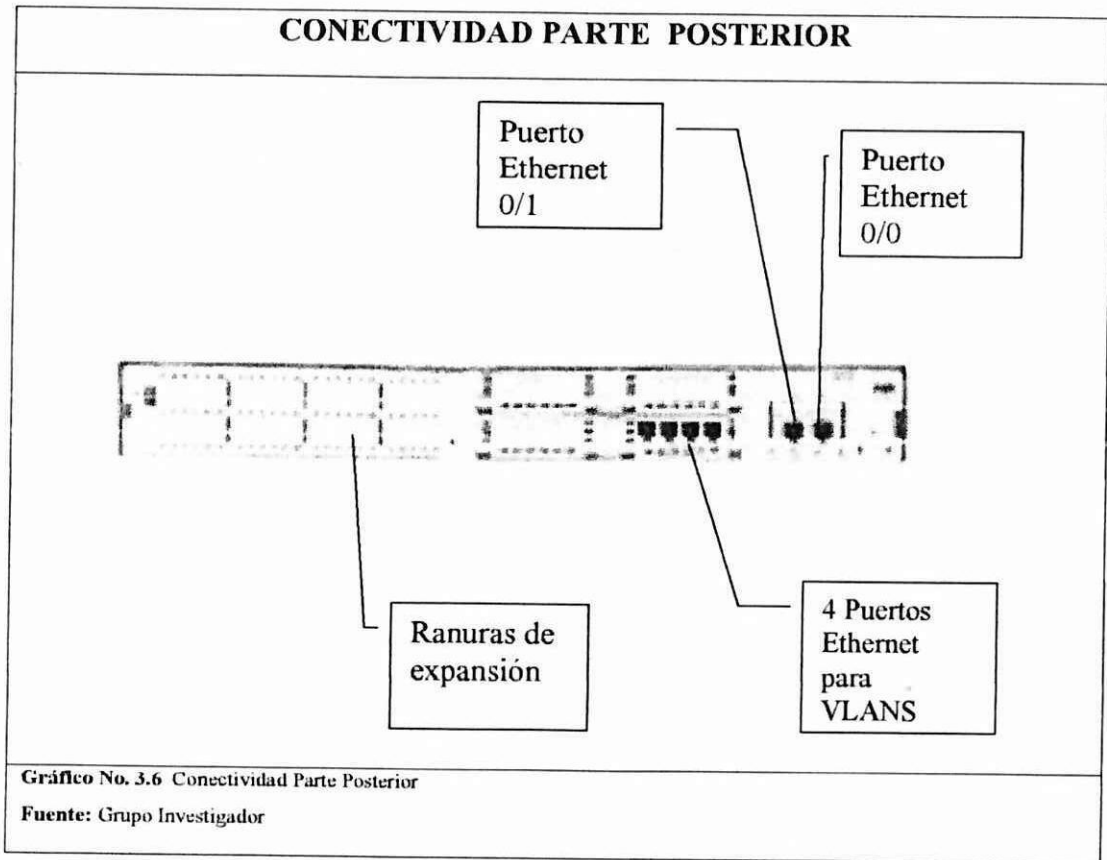


Gráfico No. 3.6



### 3.6.3 Instalación del SDM de CISCO

SDM es el anagrama abreviado de CISCO Router and Security Device Manager. Una herramienta de management basada en web desarrollada por CISCO. No es simplemente una interfaz web. Es una herramienta java accesible a través de un web browser.

Esta herramienta soporta un rango extremadamente amplio de Routers CISCO IOS: desde los Routers de la familia 8xx, hasta los de la serie 73xx. En la

actualidad se entrega preinstalado en todos los Routers de servicios integrados nuevos de las series 850, 870, 1800, 2800 y 3800.

Es importante mencionar que el proceso de instalación del software de SDM se ha desarrollado como soporte para el usuario ya que este sistema ya se encuentra instalado en el Router CISCO 2811 del CEYPSA y no se deberá realizar dicha instalación en este equipo.

### **3.6.3.1 Requerimientos para instalación de SDM de CISCO**

#### **Hardware**

- Mínimo un equipo Pentium 4 ó Superior
- Mínimo 128 Mb. en RAM
- Mínimo 100 Libres en espacio de Disco Duro

#### **Software**

- Sistema operativo Windows XP Professional, 2003 Server Standard Edition o 2000 Professional con Service Pack 4.
- Windows 2000 Advanced Server NO está soportado.
- Navegador de Internet Firefox 1.0.6+, Internet Explorer 5.5+ o Netscape 7.1 o 7.2.
- Habilitar el uso de ventanas emergentes.
- Sun Java Runtime Environment (JRE) versiones.
- Software de Instalación SDM Ver 2.4.1 de CISCO

### 3.6.4 Instalación de SDM de CISCO

A continuación se detalla el proceso de instalación, el mismo que sigue los siguientes pasos:

1. Ingresar a la carpeta de instalación de SDM, y ejecutar SETUP.EXE
2. Inicia el proceso de instalación, visualizando la siguiente información

Gráfico No. 3.7



3. Se presenta la pantalla de bienvenida al software de instalación. Clic en el botón siguiente para continuar con la instalación

Gráfico No. 3.8



4. El siguiente punto es aceptar la licencia de uso del software y clic en siguiente. Cabe indicar que el software es gratuito distribuido por CISCO.

Gráfico No. 3.9



5. A continuación seleccionamos el tipo de instalación a realizar, las opciones son:

Gráfico No. 3.10

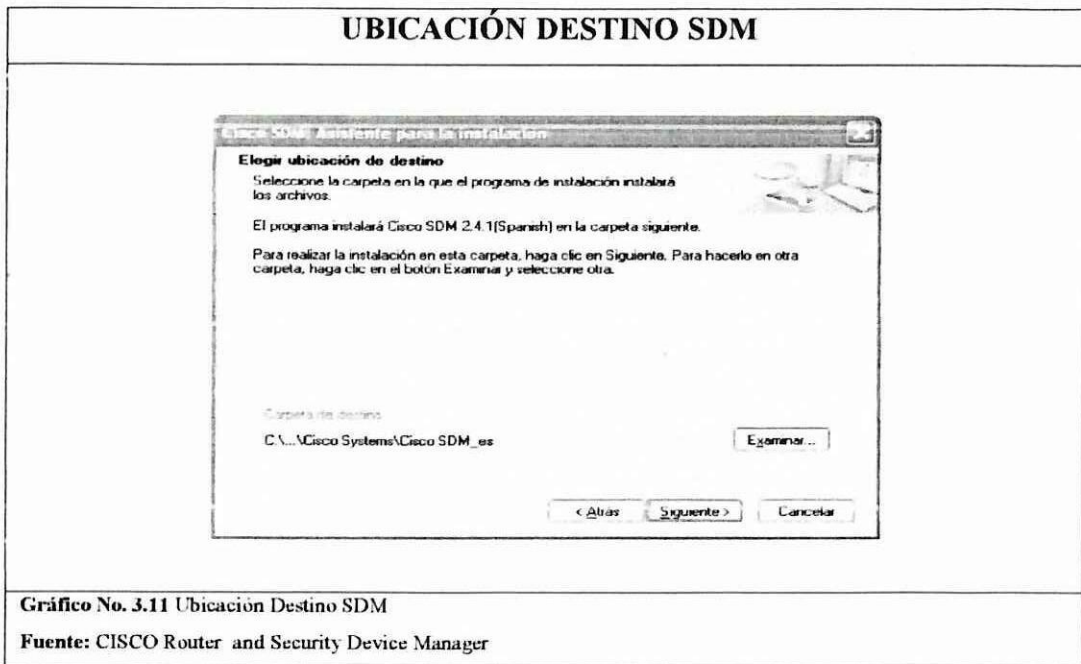


- **En este Equipo.-** Para instalar el software solamente en la estación de trabajo
- **CISCO Router.-** Para instalar el software solamente en la memoria del Router. En este caso el Router deberá estar conectado en red con la estación
- **Ambos.-** Para instalar el software tanto en la estación de trabajo como en el Router. En este caso el Router deberá estar conectado en red con la estación

Seleccionada la opción a instalar clic en siguiente

6. El siguiente paso es definir el directorio de la estación donde se instalará el software. Si no desea utilizar el que viene por defecto utilizar el botón **Examinar** para seleccionar una nueva ubicación. Definidos estos puntos clic en siguiente

Gráfico No. 3.11



7. Se presentará la pantalla para iniciar la instalación, si desea realizar cambios utilice atrás caso contrario para iniciar la instalación clic en el botón Instalar.

Gráfico No. 3.12



8. El software se instala con las opciones señaladas anteriormente. Una vez concluido se presenta la siguiente pantalla.

Gráfico No. 3.13



9. Para ingresar al software se creará un acceso en Windows como se indica a continuación.

Gráfico No. 3.14

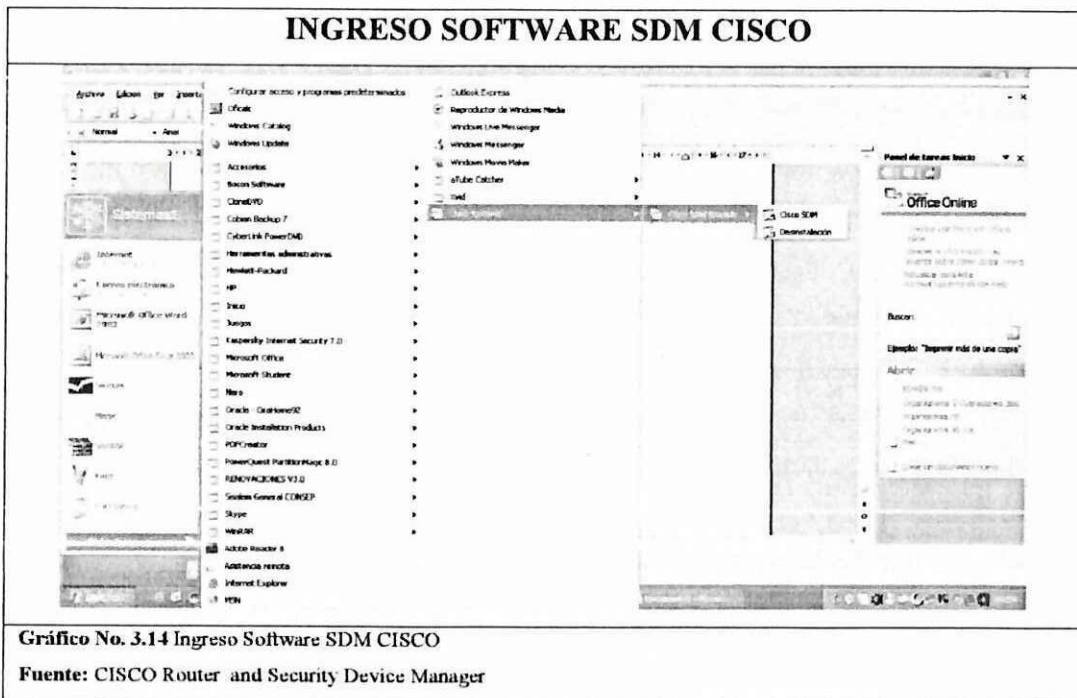


Gráfico No. 3.14 Ingreso Software SDM CISCO  
Fuente: CISCO Router and Security Device Manager

### 3.6.5 Instalación de JAVA

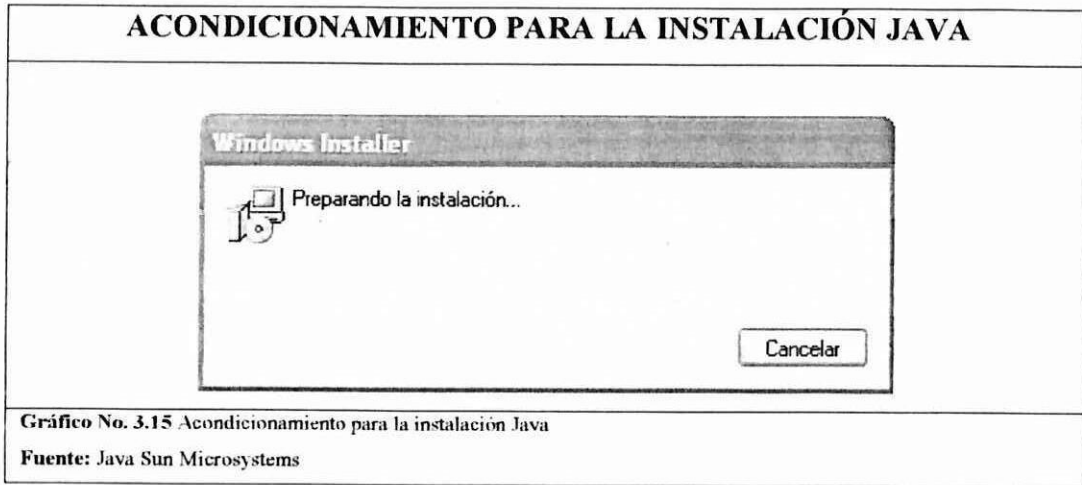
Java es una plataforma virtual de software desarrollada por Sun Microsystems, de tal manera que los programas creados en ella puedan ejecutarse sin cambios en diferentes tipos de arquitecturas y dispositivos computacionales.

Es importante dejar establecido que sin este componente instalado en el equipo que tendrá acceso al Router en modo gráfico y por lo tanto no podrá utilizar el software de SDM.

El proceso de instalación es el siguiente:

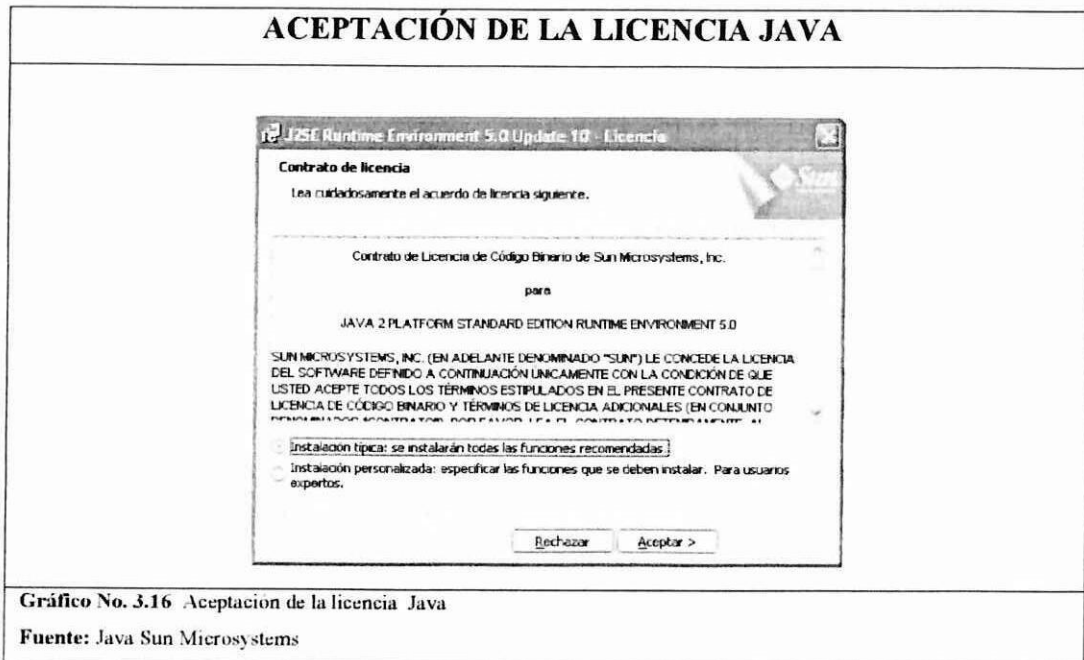
1. Ingresamos a la carpeta donde se encuentre disponible el instalador de Java y lo ejecutamos, el archivo es `java_runtime_environment_1_5_0_10.exe`
2. Se visualizará la pantalla que prepara la instalación

Gráfico No. 3.15



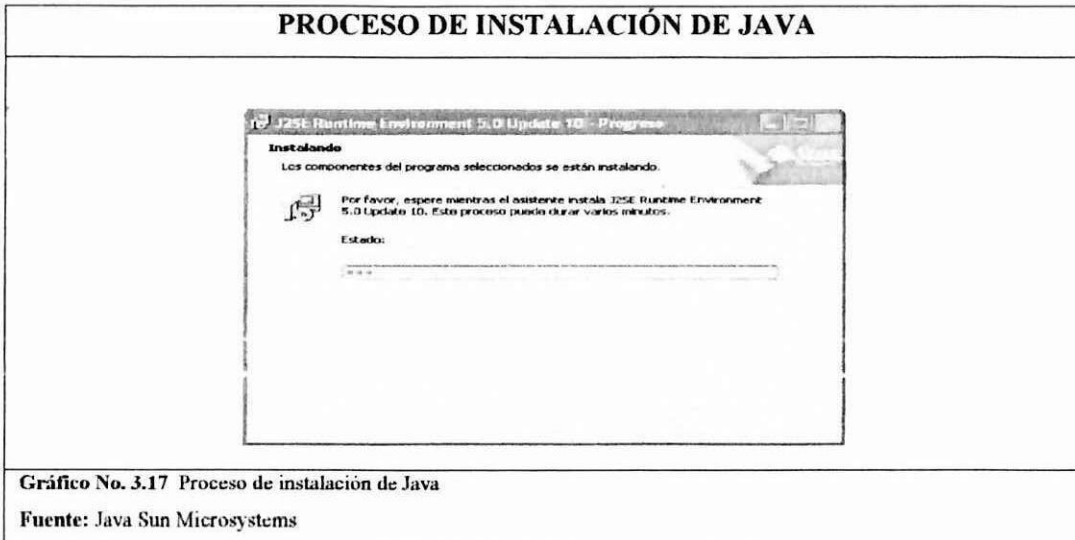
3. Completada la preparación de la instalación, se presenta la pantalla de aceptación de la licencia, hay que mencionar que es software de libre distribución; debemos seleccionar el tipo de instalación que en nuestro caso es Instalación Típica, y clic en Aceptar>

Gráfico No. 3.16



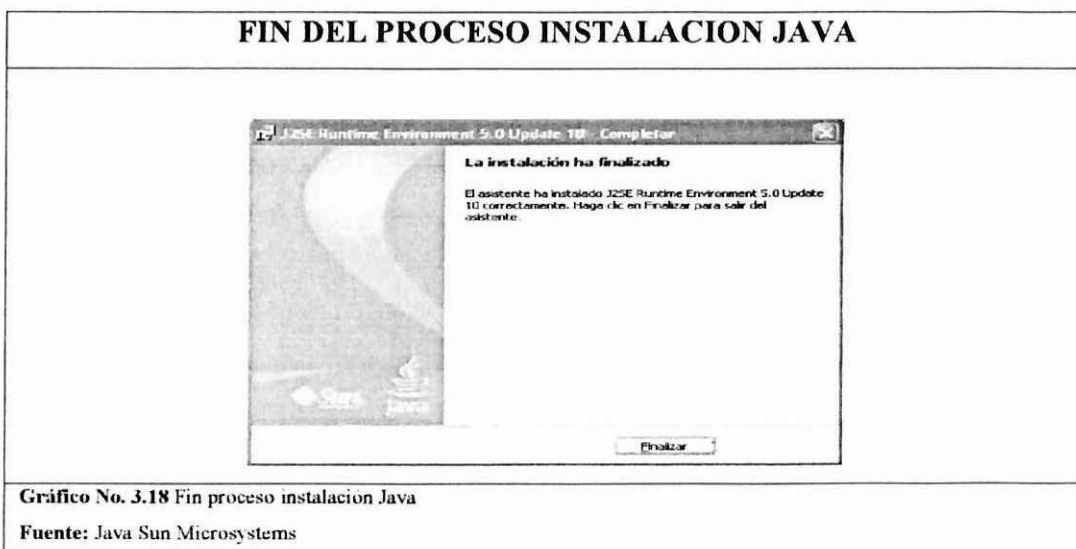
4. Inicia el proceso de instalación del software en el equipo

Gráfico No. 3.17



5. Luego del proceso de instalación se presenta la pantalla indicando el fin del proceso

Gráfico No. 3.18



## 3.7 Modos de Acceso al Router

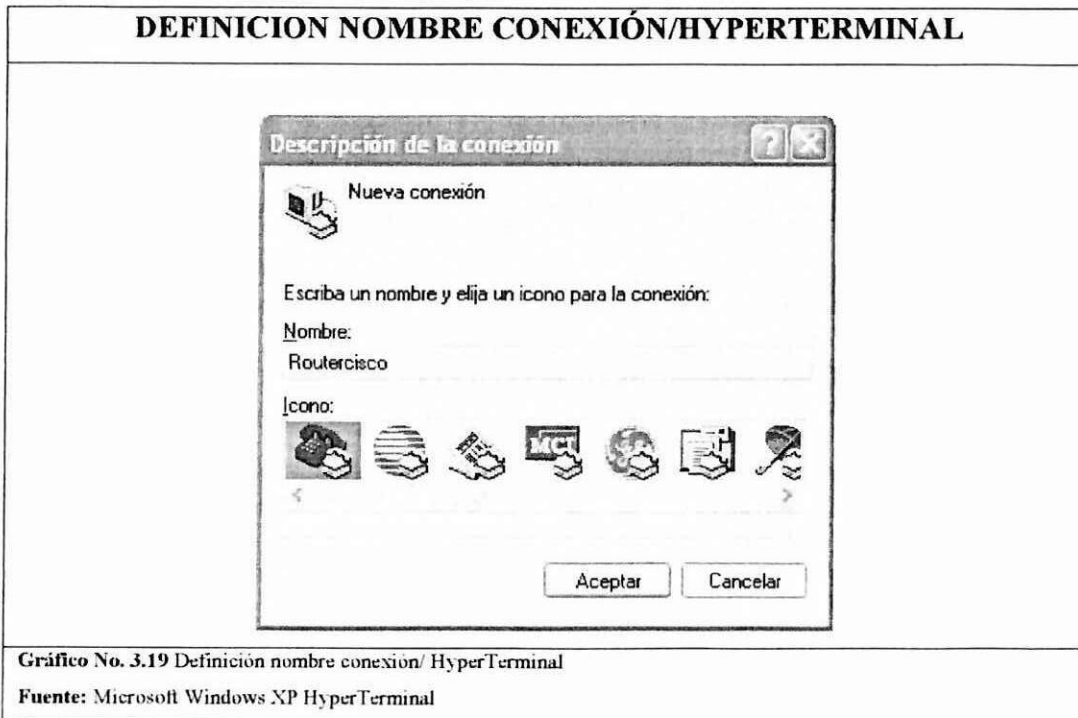
### 3.7.1 Modo Línea de Comando - EXEC

#### 3.7.1.1 Acceso al IOS

Todos los Routers tienen un puerto de consola, con cada Router se incluye un cable azul para conectar al COM del ordenador y a la boca de consola del Router, la consola del Router se abre mediante el programa HyperTerminal que incluye Windows.

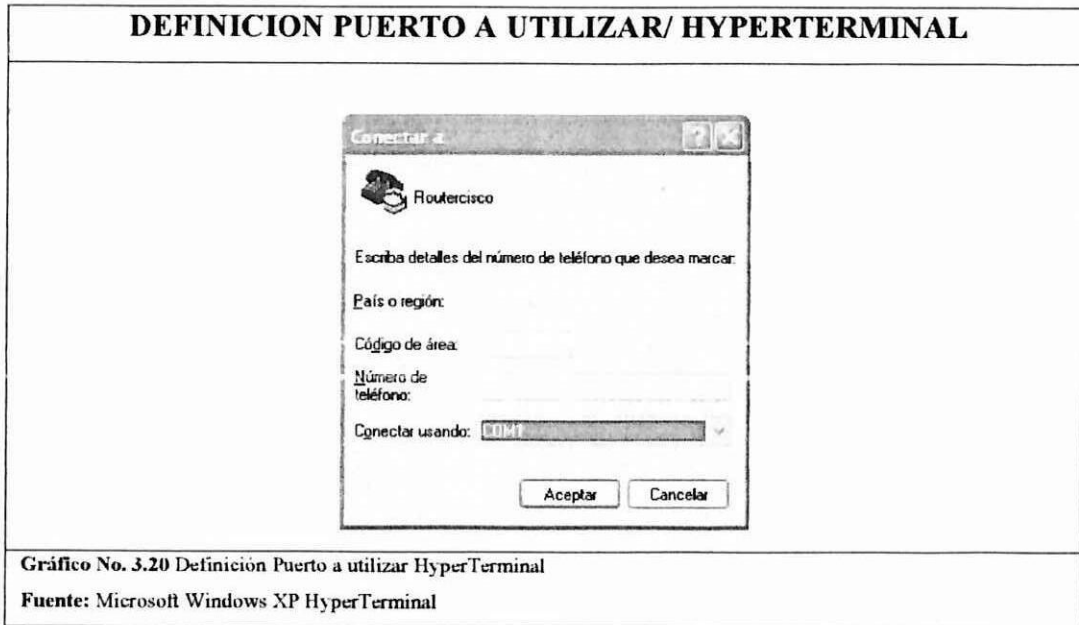
1. Una vez activado HyperTerminal definimos el nombre de la conexión

Gráfico No. 3.19



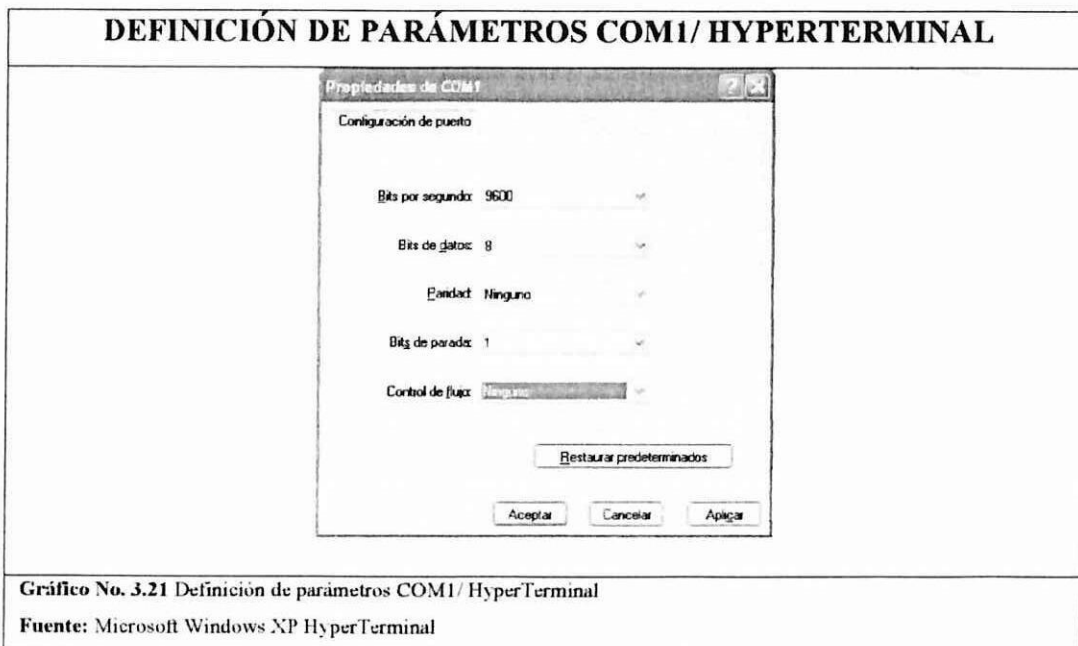
2. Se define el puerto a utilizar, en este caso COM1

Gráfico No. 3.20



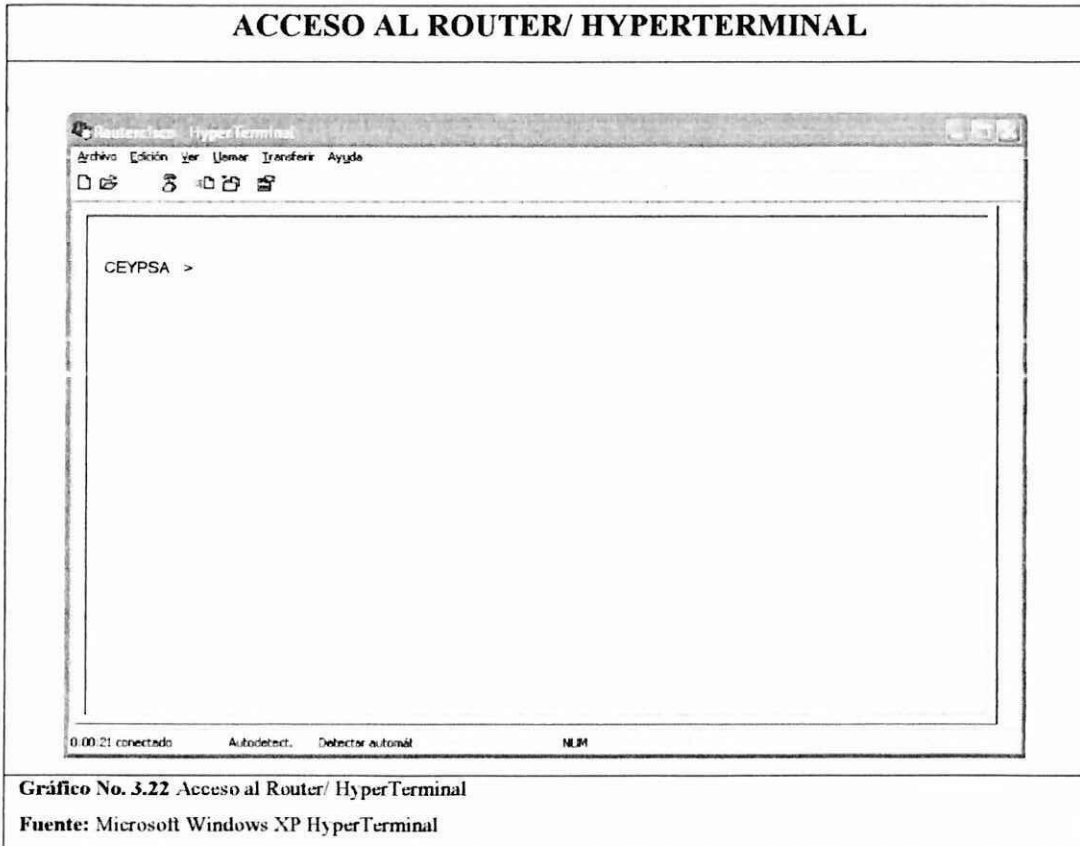
3. Se define los siguientes parámetros

Gráfico No. 3.21



4. Presionando <<Enter>> se dispone de acceso al Router

Gráfico No. 3.22



Se puede trabajar en dos modos que son:

- **Modo Usuario:** Sólo permite chequear el estado del modem, no se permiten cambios de configuración
- **Modo Privilegiado:** Permite cambiar la configuración

Consideraciones:

- Una vez lograda la conexión entre el PC y el Router , para pasar al modo privilegiado, el comando es “**enable**”
- Para pedir ayuda sobre los comandos, sólo hay que teclear “?”

- IOS reconoce los comandos con sólo escribir unas letras. ¿Cuántas? Las suficientes como para que no haya ambigüedad en los comandos

Ej: configure terminal = conf t

Ej: enable = ena

- Es posible pulsar las teclas del cursor de arriba y abajo para navegar por el histórico de comandos introducidos (también sirve Ctrl-p y Ctrl-n)

### 3.7.1.2 Comandos CISCO del Modo de Usuario

Tabla No. 3.2

<b>COMANDOS CISCO MODO USUARIO</b>	
<b>Comando</b>	<b>Descripción</b>
connect {dirección_ip nombre}	Permite conectarse remotamente a un host
disconnect conexión	Desconecta una sesión telnet establecida desde el Router
Enable	Ingresa al modo EXEC Privilegiado
Logout	Salir del modo EXEC
ping {dirección_ip nombre}	Envía una petición de eco para diagnosticar la conectividad básica de red
Resume conexión	Resume una sesión telnet interrumpida con la secuencia CTRL+SHIFT+6 y X
show cdp	Muestra el intervalo entre publicaciones CDP, tiempo de validez y versión de la publicación
show cdp entry [* nombre_dispositivo] [protocol version]}	Muestra información acerca de un dispositivo vecino registrado en una tabla CDP
show cdp interfaces [tipo número]	Muestra información acerca de las interfaces en las que CDP está habilitado

show cdp neighbors [tipo número] [detail]	Muestra los resultados del proceso de descubrimiento de CDP
show clock	Muestra la hora y fecha del Router
show history	Muestra el historial de comandos ingresados
show hosts	Muestra una lista en caché de los nombres de host y direcciones
show ip interface brief	Muestra un breve resumen de la información y del estado de una dirección IP
show ip rip database	Muestra el contenido de la base de datos privada de RIP
show ip route [dirección  protocolo]	Muestra el contenido de la tabla de enrutamiento IP. El parámetro dirección permite acotar la información que se desea visualizar, exclusivamente a la dirección ingresada. El parámetro protocolo permite indicar la fuente de aprendizaje de las rutas que se desean visualizar, como por ejemplo rip, igmp, static y connected
show sessions	Muestra las conexiones Telnet establecidas en el Router
show version	Muestra información sobre el CISCO IOS y la plataforma
telnet {dirección_ip nombre}	Permite conectarse remotamente a un host
terminal editing	Reactiva las funciones de edición avanzada
terminal history size numero_líneas	Establece el tamaño del buffer del historial de comandos
terminal no editing	Deshabilita las funciones de edición avanzada
traceroute dirección_ip	Muestra la ruta tomada por los paquetes hacia un destino
<p><b>Tabla No. 3.2</b> Comandos CISCO Modo usuario</p> <p><b>Fuente:</b> Simulador BOSON NET SIMM FOR CCNP</p>	

### 3.7.1.3 Comandos CISCO Modo EXEC Privilegiado

Tabla No. 3.3

<b>COMANDOS CISCO MODO PRIVILEGIADO</b>	
<b>Comando</b>	<b>Descripción</b>
clear cdp counters	Restaura los contadores de tráfico CDP a cero
clear cdp table	Elimina la tabla CDP de información de los vecinos
clear counters	Despeja los contadores de las interfaces
configure memory	Carga información de configuración de la NVRAM
configure Terminal	Configura la terminal manualmente desde la terminal de consola
copy flash tftp	Copia la imagen del sistema desde la memoria Flash a un servidor TFTP
copy running-config startup-config	Guarda la configuración activa en la NVRAM
copy running-config tftp	Almacena la configuración activa en un servidor TFTP
copy tftp flash	Descarga una nueva imagen desde un servidor TFTP en la memoria Flash
copy tftp running-config	Carga la información de configuración desde un servidor TFTP
Debug cdp adjacency	Muestra información recibida de vecinos CDP
Debug cdp events	Muestra información sobre eventos CDP
Debug cdp ip	Muestra información CDP específica de IP
Debug cdp packets	Muestra información relacionada a los paquetes CDP
Debug ip igrp events	Muestra todos los eventos IGRP que se están

	enviando y recibiendo en el Router.
debug ip igrp transactions	Muestra las actualizaciones IGRP que se están enviando y recibiendo en el Router
Debug ip rip	Muestra información sobre las actualizaciones de enrutamiento RIP mientras el Router las envía y recibe
Debug ip rip [events]	Muestra las actualizaciones de enrutamiento RIP a medida que se las envía y recibe
Disable	Salir del modo EXEC Privilegiado hacia el modo EXEC Usuario
erase flash	Borra el contenido de la memoria Flash
erase startup-config	Borra el contenido de la NVRAM
no debug all	Desactiva todas las depuraciones activadas en el dispositivo
Reload	Reinicia el Router
Setup	Entra a la facilidad de Diálogo de configuración inicial
show access-lists [Nro_ACL][Nom-bre_ACL]	Muestra el contenido de todas las ACL en el Router. Para ver una lista específica, agregue el nombre o número de ACL como opción a este comando
show arp	Muestra la asignación de direcciones IP a MAC a Interfaz del Router
show cdp traffic	Muestra los contadores CDP, incluyendo el número de paquetes enviados y recibidos, y los errores de checksum
show controllers serial [número]	Muestra información importante como que tipo de cable se encuentra conectado
show debugging	Muestra información acerca de los tipos de depuraciones que están habilitados
show flash	Muestra la disposición y contenido de la memoria Flash

show interfaces [tipo número]	Muestra estadísticas para la/las interfaces indicadas
show ip interface [tipo número]	Muestra los parámetros de estado y globales asociados con una interfaz
show ip protocols [summary]	Muestra los parámetros y estado actual del proceso de protocolo de enrutamiento activo
show memory	Muestra estadísticas acerca de la memoria del Router , incluyendo estadísticas de memoria disponible
show processes	Muestra información acerca de los procesos activos
show protocols	Muestra los protocolos de capa 3 configurados
show running-config	Muestra la configuración actual en la RAM
show sessions	Muestra las conexiones Telnet establecidas en el Router
show stacks	Controla el uso de la pila de procesos y rutinas de interrupción y muestra la causa del último re arranque del sistema
show startup-config	Muestra la configuración que se ha guardado, que es el contenido de la NVRAM
terminal monitor	Si se utiliza una sesión por telnet para examinar el Router , entonces, permite redirigir el resultado y los mensajes del sistema hacia a terminal remota
undebug all	Desactiva todas las depuraciones activadas en el dispositivo

**Tabla No. 3.3** Comandos CISCO Modo Privilegiado

**Fuente:** Simulador BOSON NET SIMM FOR CCNP

### 3.7.1.4 Comandos CISCO Modo de Configuración Global

Tabla No. 3.4

COMANDOS CISCO MODO DE CONFIGURACIÓN GLOBAL	
Comando	Descripción
access-list Nro_ACL {permit deny} Origen	Crea o agrega una sentencia de condición a la ACL que permitirá o denegará los paquetes que llegan desde un Origen. Este último parámetro puede ser una dirección IP más una máscara wildcard, la palabra host más una dirección IP o el wildcard any
access-list Nro_ACL {permit deny} Proto Origen Destino [Operador Nro_puerto] [established][echo  echo- reply]	Crea o agrega una sentencia de condición a la ACL que permitirá o denegará los paquetes que lleguen desde un Origen y vayan hacia un Destino. Proto identifica el protocolo a verificar. Origen y Destino pueden ser una dirección IP más una máscara wildcard, la palabra host más una dirección IP o el wildcard any. Operador puede ser lt (menor que), gt (mayor que), eq (igual a) o neq (distinto a). Nro_puerto indica el puerto TCP o UDP. El parámetro established permite el paso de tráfico cuando hay una sesión establecida. En el caso del protocolo ICMP se puede utilizar echo o echo-reply.
Banner motd #mensaje del día#	Configura un cartel con un mensaje del día. Ej: banner motd #Bienvenido#
boot system flash [nombre_imagen_IOS]	Especifica que el Router cargue el IOS desde la Flash Ej: boot system flash c2500-IOS
boot system rom	Especifica que el Router cargue el IOS desde la ROM

boot system tftp nombre_imagen_IOS dir_IP_server_tftp	Especifica que el Router cargue el IOS desde un servidor TFTP. Ej: boot system tftp c2500-IOS 24.232.150.1
cdp run	Habilita CDP globalmente en el Router
clock set hh:mm:ss mes día año	Modificar la fecha y hora del Router. Ej: clock set 12:31:00 July 12 2004
config-register valor_registro_configuración	Cambia los valores del registro de configuración. Ej: config-register 0x2142
Enable password contraseña	Establece una contraseña local para controlar el acceso a los diversos niveles de privilegio. Ej: enable password class
Enable secret contraseña	Especifica una capa de seguridad adicional mediante el comando enable password. Ej: enable secret class
hostname nombre	Modifica el nombre del Router. Ej: hostname Lab_A
interface tipo número	Configura un tipo de interfaz y entra al modo de configuración de interfaz. Ej: interface ethernet 0
ip access-list {[standard extended] Nombre	Permite crear una ACL nombrada. Se debe indicar el tipo. Este comando ingresa al Router al submodo de configuración que puede reconocerse por el prompt Router (config-ext-nacl)#
ip classless	Permite que el Router no tome en cuenta los límites con definición de clases de las redes en su tabla de enrutamiento y simplemente transmita hacia la ruta por defecto
ip default-network dirección_red	Establece una ruta por defecto. Ej: ip default-network 210.32.45.0
ip domain-lookup	Habilita la conversión de nombre a dirección en

	el Router
ip host nombre_host dir_ip1 .... Dir_ip8	Crea una entrada de nombre a dirección estática en el archivo de configuración del Router. Ej: ip host Lab_A 192.168.5.1 210.110.11.1
ip http Server	Permite que el Router actúe como servidor Web http limitado
ip name-server dir_ip1 .... Dirip6	Especifica las direcciones de hasta seis servidores de nombres para su uso para la resolución de nombres y direcciones.
Ip route dirección_red máscara dir_ip_salto [distancia_administrativa]	Establece rutas estáticas. Ej: ip route 210.42.3.0 255.255.255.0 211.1.2.1
line tipo número	Identifica una línea específica para la configuración e inicia el modo de reunión de comandos de configuración. Ej: line console 0 ó line vty 0 4
Router protocolo_de_enrutamiento [nro_AS]	Inicia un proceso de enrutamiento definiendo en primer lugar un protocolo de enrutamiento IP. Ej: Router rip ó Router igrp 120
service password-encryption	Habilita la función de cifrado de la contraseña
<b>Tabla No. 3.4 Comandos CISCO Modo de Configuración Global</b> <b>Fuente:</b> Simulador BOSON NET SIMM FOR CCNP	

### 3.7.1.5 Comandos CISCO Submodo de Configuración de Interfaz

Tabla No. 3.5

<b>COMANDOS CISCO SUBMODO DE CONFIGURACIÓN INTERFAZ</b>	
<b>Comando</b>	<b>Descripción</b>
bandwidth Kbps	Establece un valor de ancho de banda para una interfaz. Ej: bandwidth 64

cdp enable	Habilita CISCO Discovery Protocol en una interfaz
cdp holdtime segundos	Especifica el tiempo de espera antes de ser enviada la siguiente actualización CDP
cdp timer segundos	Especifica la frecuencia con que son enviadas actualizaciones CDP
clock rate velocidad	Configura la velocidad de reloj para las conexiones de hardware en interfaces seriales, como módulos de interfaz de red y procesadores de interfaz a una velocidad de bits aceptable. Ej: clock rate 56000
description descripción	Agrega una descripción a la interfaz. Ej: description Conectada a Internet
ip access-group Nro_ACL [in out]	Asigna la ACL indicada a la interfaz, ya sea para que verifique los paquetes entrantes (in) o los salientes (out)
ip address dirección_ip mascara_red	Asigna una dirección y una máscara de subred e inicia el procesamiento IP en una interfaz. Ej: ip address 192.168.52.1 255.255.255.0
No ip route-cache	Para deshabilitar el balanceo de carga por destino, que esté habilitado por defecto
No ip split-horizon	Deshabilita el horizonte dividido en la interfaz, que por defecto se encuentra habilitado. Para volver habilitarlo utilice el comando ip split-horizon
No shutdown	Reinicia una interfaz desactivada
Shutdown	Inhabilita una interfaz
<b>Tabla No. 3.5 Comandos CISCO Submodo de Configuración Interfaz</b> <b>Fuente:</b> Simulador BOSON NET SIMM FOR CCNP	

### 3.7.1.6 Comandos CISCO Submodo de Configuración de Línea

Tabla No. 3.6

<b>COMANDOS CISCO SUBMODO DE CONFIGURACIÓN DE LINEA</b>	
<b>Comando</b>	<b>Descripción</b>
access-class Nro_ACL in	En las líneas VTY, asigna una lista de control de acceso a las conexiones establecidas via Telnet
Login	Habilita la verificación de contraseña en el momento de la conexión.
password contraseña	Asigna la contraseña a ser solicitada en el momento de la conexión

**Tabla No. 3.6** Comandos CISCO Submodo de Configuración de Línea  
**Fuente:** Simulador BOSON NET SIMM FOR CCNP

### 3.7.1.7 Comandos CISCO de Edición y otros

Tabla No. 3.7

<b>COMANDOS CISCO DE EDICION Y OTROS</b>	
<b>Teclas / Comando</b>	<b>Descripción</b>
Ctrl+A	Permite desplazarse al principio de la línea de comandos
Esc+B	Permite desplazarse una palabra hacia atrás
Ctrl+B (o Flecha Izquierda)	Permite desplazarse un carácter hacia atrás
Ctrl+E	Permite desplazarse hasta el final de la línea de comandos
Ctrl+F (o Flecha Derecha)	Permite desplazarse un carácter hacia delante
Ctrl+P (o Flecha Arriba)	Muestra el último comando ingresado
Ctrl+N (o Flecha Abajo)	Muestra el comando más reciente

<Tab> (tecla Tabulador)	Completa el comando ingresado parcialmente
Ctrl+Z (o end)	Estando en cualquier modo de configuración regresa al modo EXEC Privilegiado
Ctrl+C	Cancela la ejecución del Dialogo de configuración inicial o Setup
Ctrl+Shift+6	Permite interrumpir intentos de ping, traceroute y traducciones de nombres
Exit	Estando en el modo de configuración global o cualquiera de sus submodos regresa al modo anterior. Estando en los modos EXEC Usuario o EXEC Privilegiado, cierra la sesión
<b>Tabla No. 3.7</b> Comandos CISCO de edición y otros <b>Fuente:</b> Simulador BOSON NET SIMM FOR CCNP	

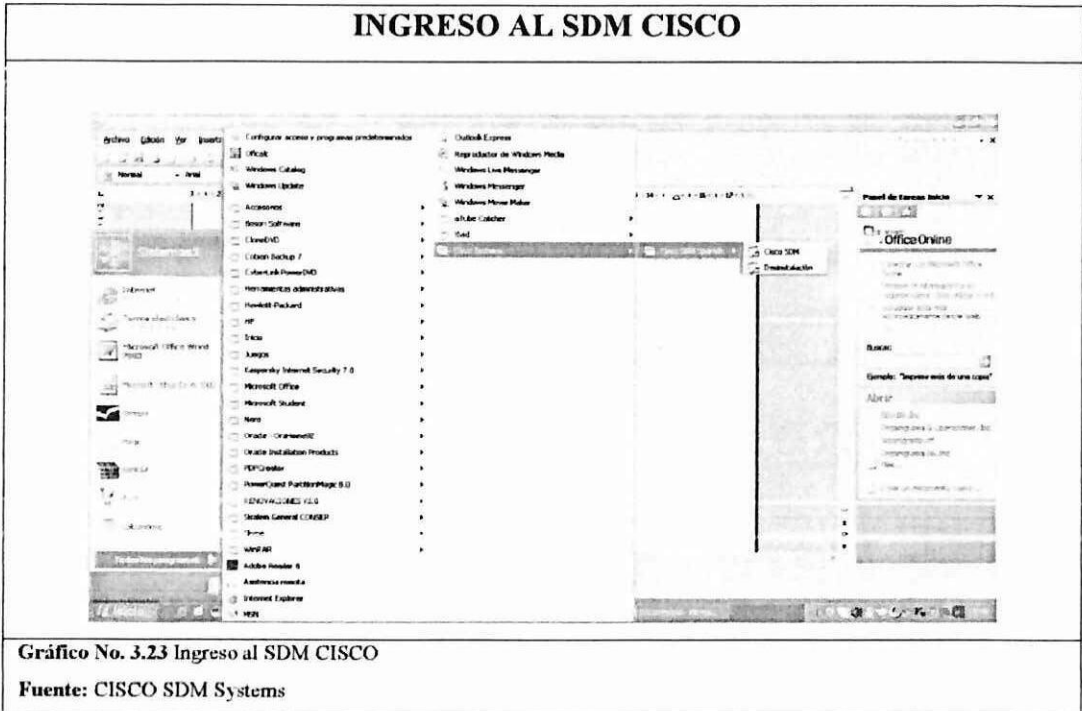
### 3.7.2 Modo Grafico – SDM

#### 3.7.2.1 Acceso SDM

El acceso a la configuración en modo gráfico mediante la utilización de SDM de CISCO se la puede realizar de dos formas, las mismas que son:

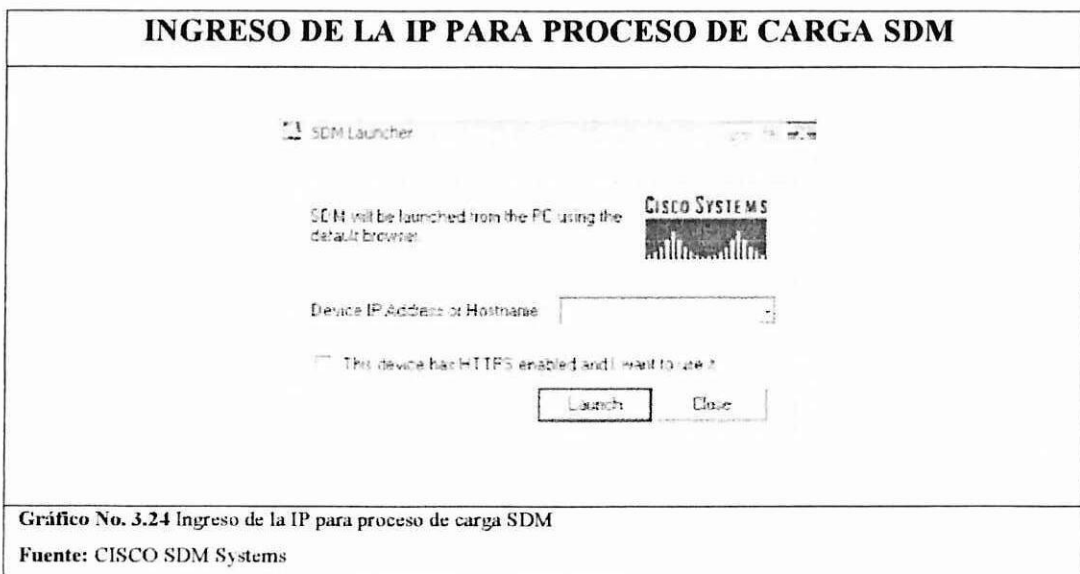
1. Ingresamos al software a través del acceso creado en la instalación

Gráfico No. 3.23



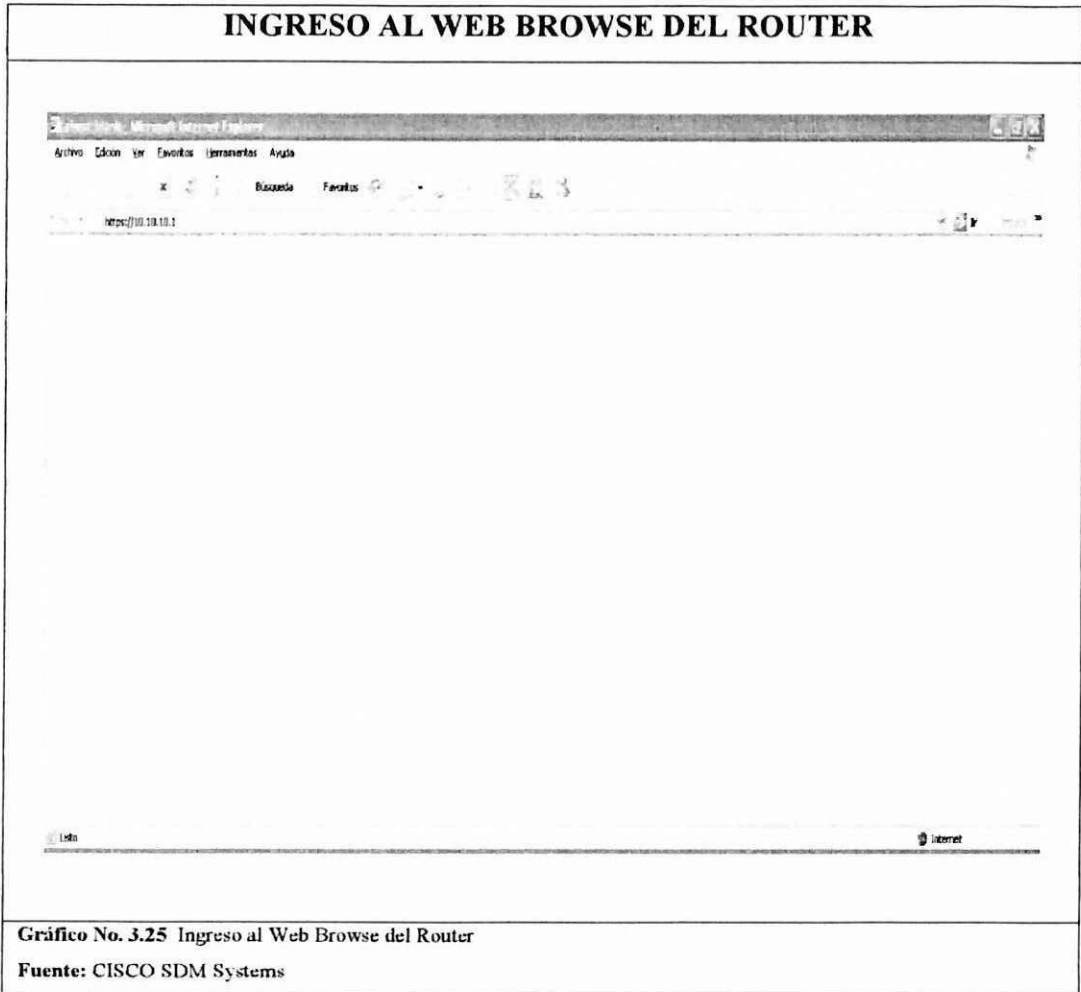
Se abrirá una ventana de diálogo requiriendo el ingreso de la dirección IP del dispositivo. Ingrese la IP del dispositivo e inmediatamente se abrirá una ventana del navegador de Internet para comenzar el proceso de carga.

Gráfico No. 3.24



2. Ingresar al web browse y digitar la dirección IP del Router , en el caso del CEYPSA la dirección IP es <https://10.10.10.1>

Gráfico No. 3.25



En ambos casos se inicia el proceso de acceso a la información del Router mostrándose las siguientes pantallas.

Gráfico No. 3.26

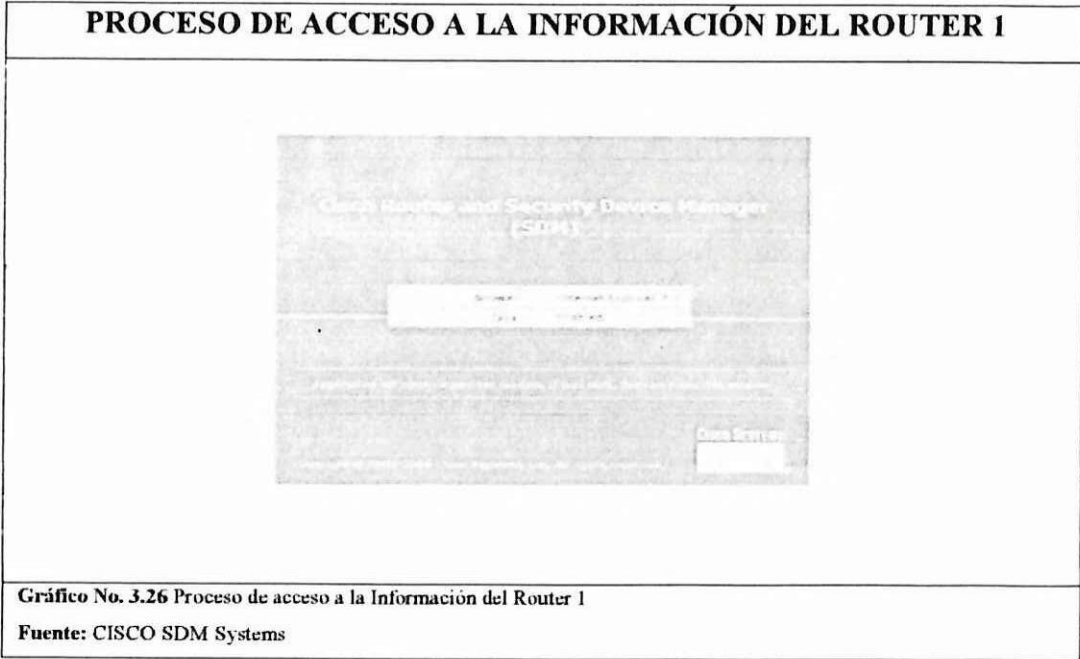
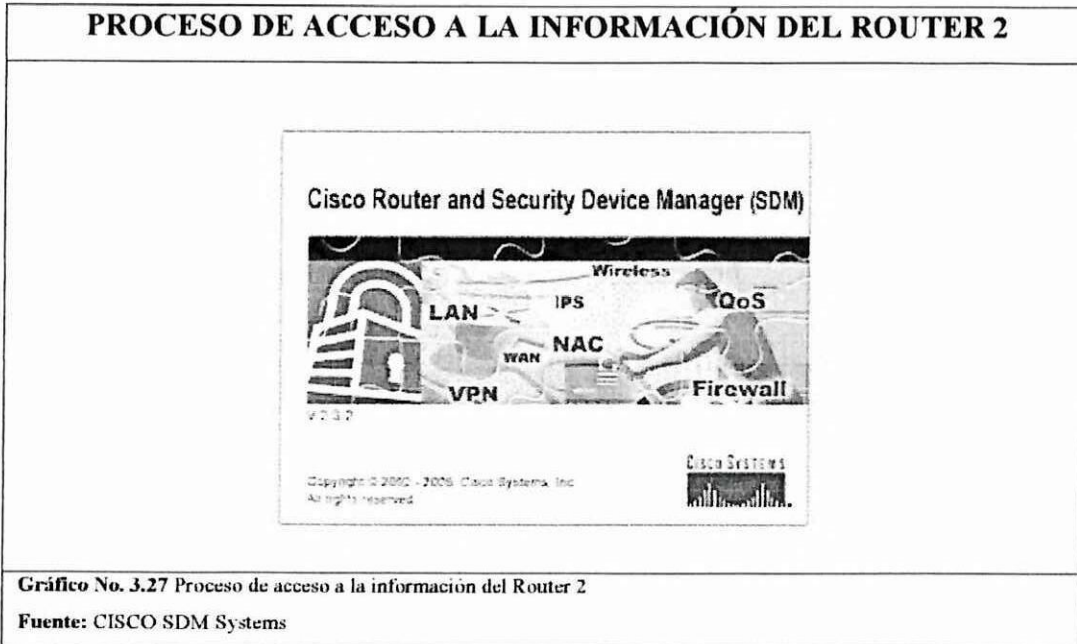


Gráfico No. 3.27



Como siguiente punto debemos ingresar el usuario y la clave para poder acceder a la configuración del equipo.

## 3.8 Información del Router CEYPSA

### 3.8.1 Pantalla de Información General

Gráfico No. 3.28

**INFORMACIÓN GENERAL DEL ROUTER CEYPSA**

**Propiedades del router**

Nombre de host: CEYPSA

Tipo de modelo:	Cisco 2811	Versión IOS:	12.4(11)T
Memoria disponible / total (MB):	158/256 MB	Versión SDM:	2.4.1
Capacidad de flash total:	122 MB		

**Resumen general de configuración**

LAN totales admitidas:	7	WAN totales admitidas:	0
Interfaz de LAN configurada:	7	Conexiones WAN totales:	0
Servidor DHCP:	No configurado		
IPSec (sitio a sitio):	0	GRE sobre VPN IPSec:	0
Conexión a Xauth necesaria:	0	Easy VPN remoto:	0
Nº de clientes DMVPN:	0	Nº de clientes VPN activos:	0
Nº de rutas estáticas:	2	No se admite IPS	
Protocolos de enrutamiento dinámico:	Ninguna		

Gráfico No. 3.28 Información General del Router CEYPSA  
Fuente: CISCO SDM Systems

#### Menú de opciones

- **Inicio.-** Permite visualizar la pantalla general de estadísticas del Router

- **Configurar.-** Ingresa al modo de configuración del Router, en la cual se puede realizar entre otras las siguientes tareas: Parámetros de cada de las interfaces Ethernet, serial, etc. Configurar el Firewall y Listas de Control de Acceso. Parámetros de la Red Privada Virtual. Seguimiento a través de la Auditoria de Seguridad. Configurar el Enrutamiento. Definir las características del Network Address Translation. Es un standard de Internet que le permite a una red local (LAN) usar un grupo de direcciones de IP para el tráfico (NAT). Determinar como se va a realizar la Prevención de Intrsiones.
- **Monitor.-** Visualiza el a través de gráficas todo el funcionamiento actual del Router
- **Actualizar.-** Refresca toda la información que se visualiza de acuerdo a lo que este realizando el Router
- **Guardar.-** Permite almacenar los cambios realizados en los parámetros de configuración
- **Búsqueda.-** Opciones para buscar opciones o parámetros específicos
- **Ayuda.-** Activa el módulo de ayuda del software SDM

## 3.8.2 Información Estadística del Router

### 3.8.2.1 Opción de Configuración

Gráfico No. 3.29

**OPCION DE CONFIGURACION DEL ROUTER CEYPSA**

Interfaz	IP	Tipo	Ranura	Estado	Descripción
FastEthernet0/1	201.218.38.67	10/100 Ethernet	0	<input type="radio"/>	Haci WAN
FastEthernet0/0/0	no aplicable	Ethernet Switch Port	0	<input type="radio"/>	Haci Oficina
FastEthernet0/0/1	no aplicable	Ethernet Switch Port	0	<input type="radio"/>	Haci Administracion
FastEthernet0/0/2	no aplicable	Ethernet Switch Port	0	<input type="radio"/>	Haci Salas
FastEthernet0/0/3	no aplicable	Ethernet Switch Port	0	<input type="radio"/>	Haci Wireless
Null0	sin dirección IP	Null		<input type="radio"/>	Haci
Vlan1	10.100.100.1	Vlan		<input type="radio"/>	Haci
Vlan10	10.10.10.1	Vlan		<input type="radio"/>	Haci Oficina
Vlan20	10.10.20.1	Vlan		<input type="radio"/>	Haci Administracion
Vlan30	10.10.30.1	Vlan		<input type="radio"/>	Haci Salas
Vlan40	10.10.40.1	Vlan		<input type="radio"/>	Haci Wireless

Nombre de elemento	Valor de elemento
NAT	Interna
Regla de acceso - entrante	<Ninguno>
Regla de acceso - saliente	<Ninguno>
Política IPsec	<Ninguno>
Regla de inspección - entrante	<Ninguno>
Regla de inspección - saliente	<Ninguno>
Easy VPN remoto	<Ninguno>
Política de QoS - saliente	<Ninguno>
Política de QoS - entrante	<Ninguno>

Gráfico No. 3.29 Opción de configuración del Router CEYPSA

Fuente: CISCO SDM Systems

1. Opciones de configuración del Router
2. Menú de trabajo, se tiene entre otras las opciones:
  - Agregar.- Permite incrementar un elemento a la lista
  - Editar.- Permite la modificación de los parámetros establecidos para cada elemento.
  - Eliminar.- Quitar un elemento de la lista
  - Resumen.- Visualiza los parámetros programados en el elemento seleccionado

- Detalle.- Visualiza en detalle los parámetros programados en el elemento seleccionado
  - Desconectar.- Desactivar el elemento seleccionado
  - Probar conexión.- Permite realizar un diagnóstico de funcionamiento del elemento seleccionado
3. Muestra la cabecera de la cada uno los elementos que consta el equipo
  4. Despliega la información relacionada con el elemento seleccionado en la cabecera.

### 3.8.3 Configuración de las Interfaces del Router CEYPSA

Gráfico No. 3.30

**CONFIGURACIÓN DE LAS INTERFACES ROUTER CEYPSA**

The screenshot displays the Cisco SDM configuration interface. At the top, there's a menu bar with 'Archivo', 'Editar', 'Ver', 'Herramientas', and 'Ayuda'. Below the menu, there are tabs for 'Inicio', 'Configurar', 'Monitor', 'Actualizar', 'Guardar', 'Búsqueda', and 'Ayuda'. The main content area is titled 'Editar interfaz / conexión' and contains a table of interfaces.

Interfaz	IP	Tipo	Ranura	Estado	Descripción
FastEthernet0/0	201.219.38.87	10/100Ethernet	0	<input type="checkbox"/>	Haci WAN
FastEthernet0/0	no aplicable	Ethernet Switch Port	0	<input type="checkbox"/>	Haci Oficina
FastEthernet0/1	no aplicable	Ethernet Switch Port	0	<input type="checkbox"/>	Haci Administracion
FastEthernet0/2	no aplicable	Ethernet Switch Port	0	<input type="checkbox"/>	Haci Salas
FastEthernet0/3	no aplicable	Ethernet Switch Port	0	<input type="checkbox"/>	Haci Wireless
Null0	sin dirección IP	Null		<input type="checkbox"/>	Haci
Vlan1	10.10.100.1	Vlan		<input type="checkbox"/>	Haci
Vlan10	10.10.10.1	Vlan		<input type="checkbox"/>	Haci Oficina
Vlan20	10.10.20.1	Vlan		<input type="checkbox"/>	Haci Administracion
Vlan30	10.10.30.1	Vlan		<input type="checkbox"/>	Haci Salas
Vlan40	10.10.40.1	Vlan		<input type="checkbox"/>	Haci Wireless

Below the table, there's a section for 'Detalles de la interfaz FastEthernet0/0'. It shows various configuration parameters and their values:

Nombre de elemento	Valor de elemento
NAT	Interna
Regla de acceso - entrante	<Ninguno>
Regla de acceso - saliente	<Ninguno>
Política IPSec	<Ninguno>
Regla de inspección - entrante	<Ninguno>
Regla de inspección - saliente	<Ninguno>
Esoy VPN remoto	<Ninguno>
Política de CoS - saliente	<Ninguno>
Política de CoS - entrante	<Ninguno>

**Gráfico No. 3.30 Configuración de las Interfaces Router CEYPSA**  
**Fuente:** CISCO SDM Systems

Permite definir cada uno de los parámetros que constara cada una de las interfaces del Router , en este caso las Fast Ethernet 0/0 y 0/1. Las Fast Ethernet 0/0/0, 0/0/1, 0/0/2 y 0/0/3. Las VLAN para cada área

### 3.8.4 Configuración del Firewall del Router CEYPSA

Gráfico No. 3.31

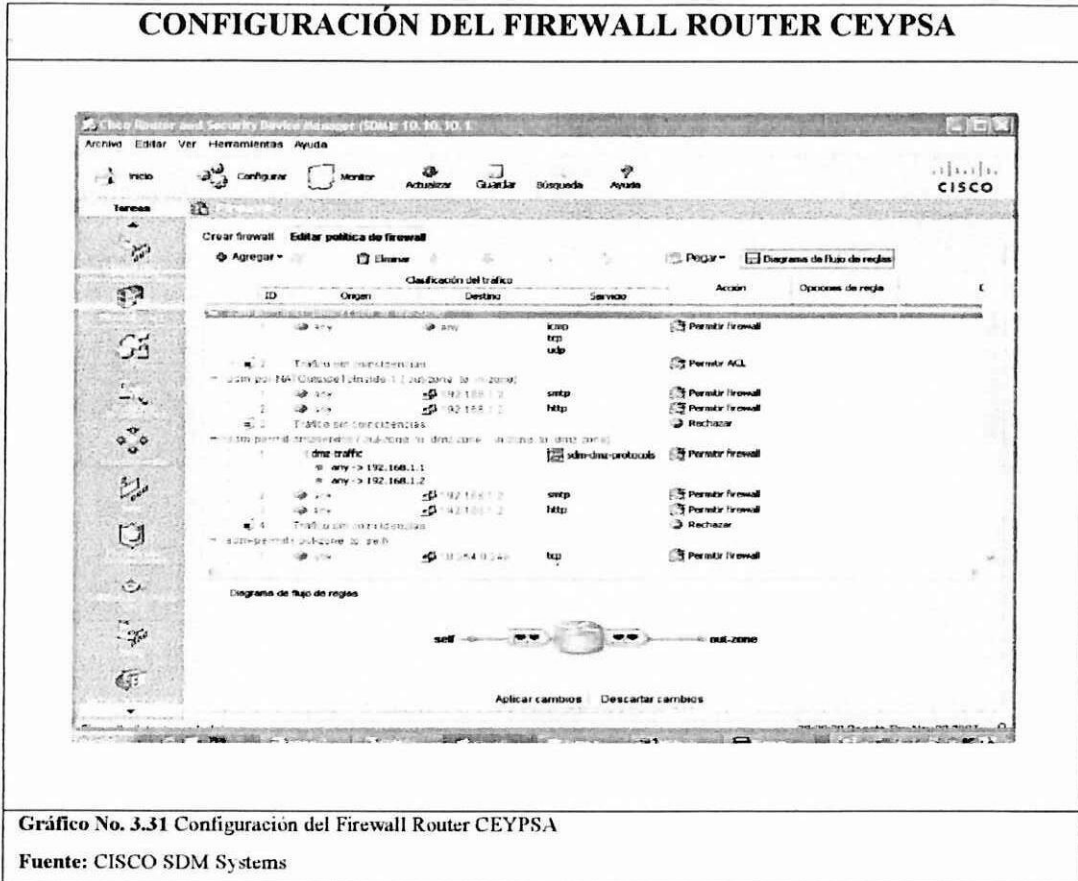


Gráfico No. 3.31 Configuración del Firewall Router CEYPSA

Fuente: CISCO SDM Systems

Se define cada una de las zonas de seguridad del equipo, las mismas que son:

1. Desde Internet hacia la red interna
2. Desde la red interna hacia Internet
3. Desde el Internet a la DMZ (Zona Desmilitarizada que es la zona física detrás de un servidor de seguridad de Internet y delante de un servidor de seguridad de segundo nivel que protege los sistemas y datos del servidor)
4. Desde la DMZ hacia el Internet

Determinado en cada una de las zonas los protocolos que se permiten utilizar y los que va a rechazar el servidor de seguridad

### 3.8.5 Enrutamiento del Router CEYPSA

Encaminamiento (o enrutamiento) Se trata de la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad. Dado que se trata de encontrar la mejor ruta posible, lo primero será definir que se entiende por mejor ruta y en consecuencia cual es la métrica que se debe utilizar para medirla.

Gráfico No. 3.32

**ENRUTAMIENTO ROUTER CEYPSA**

Enrutamiento estático					
Red de destino	Máscara de prefijo	Envío	Distancia	Ruta permanente	Nº de se
0.0.0.0	0.0.0.0	201.219.38.65	1	No	Ninguna

Enrutamiento dinámico	
Nombre de elemento	Valor de elemento
OSPF	Desactivado
EIGRP	Desactivado

**Gráfico No. 3.32 Encaminamiento del router CEYPSA**  
**Fuente: CISCO SDM Systems**

El enrutamiento permite establecer que interfaz del Router será utilizada para la conexión al equipo del proveedor de Internet, en nuestro caso la interfaz utilizada es la FastEthernet0/1 que apunta a la dirección 201.219.38.65 del equipo del proveedor.

### **3.8.6 Configuración del NAT en el Router CEYPSA**

(Network Address Translation - Traducción de Dirección de Red) es un mecanismo utilizado por Routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

Este mecanismo en el caso del Router del CEYPSA está definido de la siguiente manera:

Gráfico No. 3.33

### CONFIGURACIÓN DEL NAT EN EL ROUTER CEYPSA

Dirección original	Dirección traducida	Tipo de regla
192.168.1.2 (25)	201.219.38.66 (25)	Estático
192.168.1.2 (80)	201.219.38.66 (80)	Estático

Clonar entrada seleccionada al agregar

**Gráfico No. 3.33** Configuración NAT Router CEYPSA  
**Fuente:** CISCO SDM Systems

- La interfaz que será traducida es la FastEthernet0/0, que contiene la dirección IP 192.168.1.2
- Toda la red interna se traduce para el tráfico a la dirección IP 201.219.38.67
- Todos los pedidos realizados desde el exterior se traduce a la dirección física 201.219.38.66 a través de los puertos 25 y 80.

### 3.8.7 Configuración de las Tareas Adicionales del Router CEYPSA

Todas las configuraciones realizadas en las diferentes opciones anteriormente indicadas se resumen en esta opción y da la posibilidad de realizar varios cambios adicionales. Las opciones se presentan en un menú desplegable y al lado izquierdo se visualiza la información de la opción seleccionada.

A continuación se presentan varias pantallas referentes a esta opción:

Gráfico No. 3.34



Gráfico No. 3.34 Tareas adicionales Router CEYPSA

Fuente: CISCO SDM Systems 1

Gráfico No. 3.35

### TAREAS ADICIONALES ROUTER CEYPSA 2

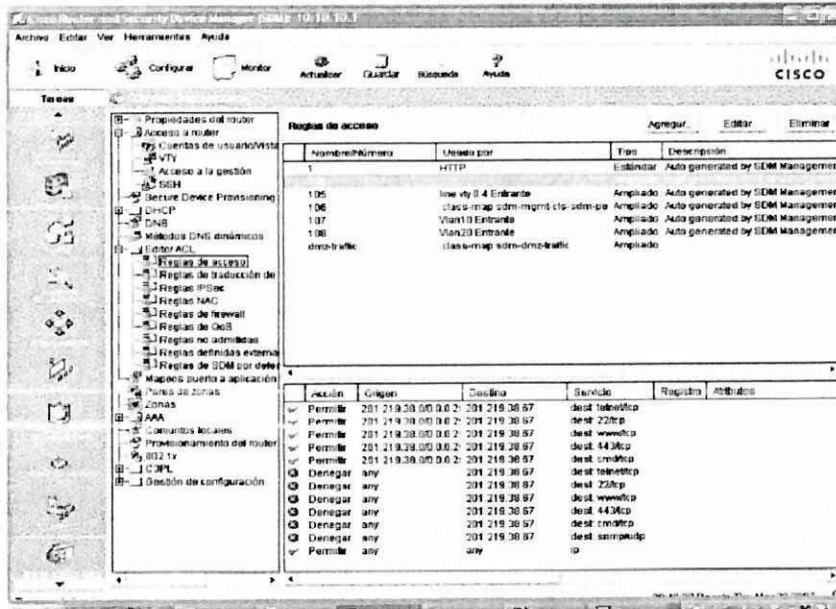


Gráfico No. 3.35 Tareas adicionales Router CEYPSA 2

Fuente: CISCO SDM Systems

Gráfico No. 3.36

### TAREAS ADICIONALES ROUTER CEYPSA 3

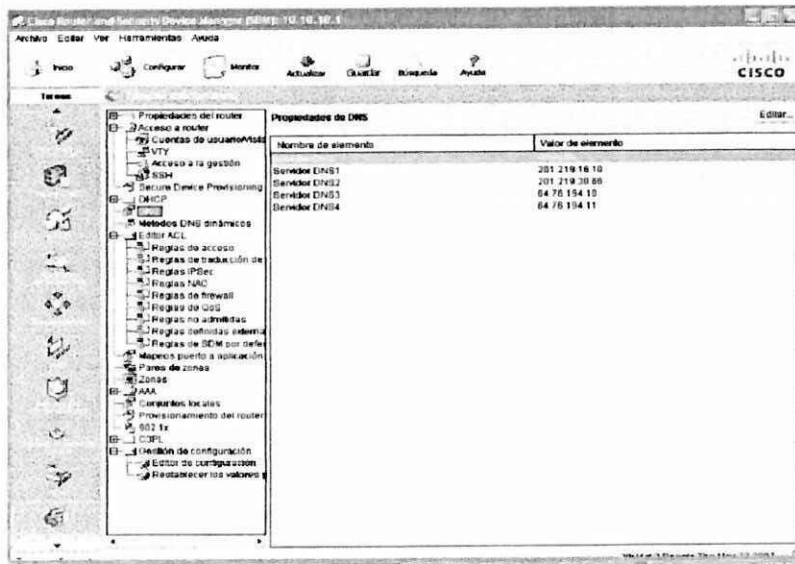


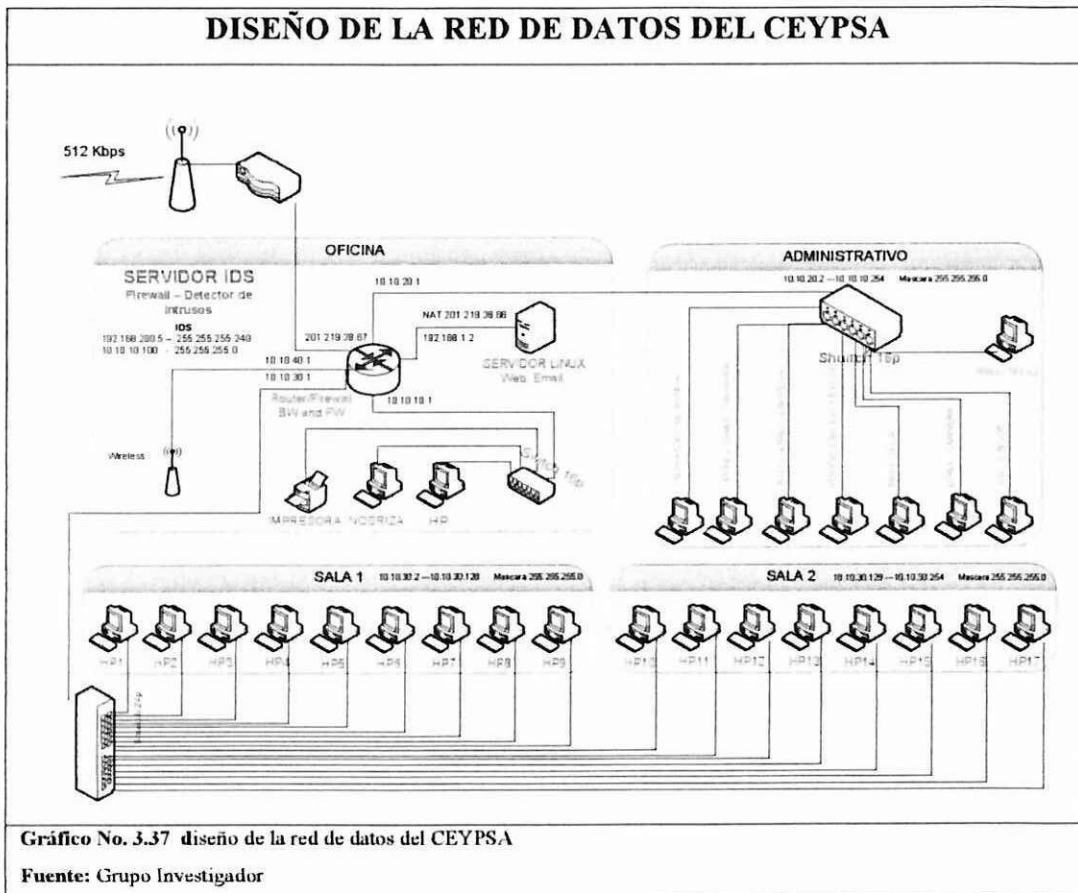
Gráfico No. 3.36 Tareas adicionales Router CEYPSA 3

Fuente: CISCO SDM Systems

### 3.9 Configuraciones del Router CISCO 2811 del Centro de Experimentación y Producción Salache

#### 3.9.1 Diseño de la Red de Datos del CEYPSA

Gráfico No. 3.37



Un vez configurado e instalado el Router CISCO 2811 en el CEYPSA la configuración queda establecida de la siguiente manera:

1. Considerando que el Router tiene 4 interfaces se han asignado de la siguiente manera:

- **FastEthernet0/0.-** Tiene la IP 192.168.1.1 para conectarle al servidor Linux que tiene la IP 192.168.1.2
- **FastEthernet0/1.-** Tiene la IP 201.219.38.67 para conectar al equipo del proveedor (antena)
- **FastEthernet0/0/0.-** Tiene la IP 10.10.10.1 asignado para la VLAN de la oficina del Administrador de la Red
- **FastEthernet0/0/1.-** Tiene la IP 10.10.20.1 asignado para la VLAN de las oficinas administrativas
- **FastEthernet0/0/2.-** Tiene la IP 10.10.30.1 asignado para la VLAN de los laboratorios
- **FastEthernet0/0/3.-** Tiene la IP 10.10.40.1 asignado para la VLAN de la red inalámbrica e edificio nuevo.

2. El diseño de la red que establecida de la siguiente manera:

- Conexión entre el servidor Linux con la interfaz 0/0 del Router , quedando asignado las direcciones IP de la siguiente manera:

Interfaz del Router : 192.168.1.1 Máscara: 255.255.255.0

Servidor Linux: 192.168.1.2 Máscara: 255.255.255.0

- Conexión con el equipo del proveedor que permite el enlace a Internet se realiza en la interfaz 0/1 del Router quedando asignado las direcciones IP de la siguiente manera:

Interfaz del Router : 201.219.35.67 Máscara: 255.255.255.248

Equipo del proveedor: 201.219.35.65 Máscara: 255.255.255.248

- VLAN de las oficinas del administrador de la red, quedando asignado las direcciones IP de la siguiente manera:

Interfaz 0/0/0 del Router : 10.10.10.1 Máscara: 255.255.255.0

IP de las estaciones: Desde la 10.10.10.2

- VLAN de las oficinas administrativas, quedando asignado las direcciones IP de la siguiente manera:

Interfaz 0/0/1 del Router : 10.10.20.1 Máscara: 255.255.255.0

IP de las estaciones: Desde la 10.10.20.2

- VLAN de los laboratorios, quedando asignado las direcciones IP de la siguiente manera:

Interfaz 0/0/2 del Router : 10.10.30.1 Máscara: 255.255.255.0

IP de las estaciones: Desde la 10.10.30.2

- VLAN del wirelles y edificio adjunto, quedando asignado las direcciones IP de la siguiente manera:

Interfaz 0/0/3 del Router : 10.10.40.1 Máscara: 255.255.255.0

IP de las estaciones: Desde la 10.10.40.2

3. La configuración de los equipos en su interfaz de red queda establecida de la siguiente manera:

VLAN 10.10.10.X

- Puerta de enlace: 10.10.10.1
- DNS Preferido: 192.168.1.2
- DNS Alternativo: 201.219.16.10

VLAN 10.10.20.X

- Puerta de enlace: 10.10.20.1
- DNS Preferido: 192.168.1.2
- DNS Alternativo: 201.219.16.10

VLAN 10.10.30.X

- Puerta de enlace: 10.10.30.1
- DNS Preferido: 192.168.1.2
- DNS Alternativo: 201.219.16.10

VLAN 10.10.40.X

- Puerta de enlace: 10.10.40.1
- DNS Preferido: 192.168.1.2
- DNS Alternativo: 201.219.16.10

### 3.10 Transformación de los Diagramas en Código.

Current configuration : 14726 bytes

!

\*\*\* Parámetros iniciales

version 12.4

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

\*\*\* definición del nombre del host

hostname CEYPSA

!

\*\*\* parámetros de arranque el Router , de donde toma la configuración de arranque

boot-start-marker

boot system flash c2800nm-advsecurityk9-mz.124-11.T.bin

boot-end-marker

!

\*\*\* establecimiento de la clave de ingreso

logging buffered 52000

enable password \*\*\*\*\*

!

```
no aaa new-model
clock timezone Bogota -5
no ip source-route
ip tcp synwait-time 10
```

```
!
```

```
!
```

```
ip cef
```

```
!
```

```
!
```

```
**** se establece las direcciones IP de los DNS
```

```
no ip bootp server
ip domain name CEYPSA.utc.edu.ec
ip name-server 201.219.16.10
ip name-server 201.219.38.66
ip name-server 64.76.194.10
ip name-server 64.76.194.11
```

```
!
```

```
multilink bundle-name authenticated
```

```
!
```

```
!
```

```
crypto pki trustpoint TP-self-signed-3911914078
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-3911914078
revocation-check none
rsa-keypair TP-self-signed-3911914078
```

```
!
```

```
!
```

```
crypto pki certificate chain TP-self-signed-3911914078
certificate self-signed 01
  30820250 308201B9 A0030201 02020101 300D0609 2A864886 F70D0101
04050030
```

31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D  
43657274  
69666963 6174652D 33393131 39313430 3738301E 170D3037 30393239  
31363330  
34355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504  
03132649  
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33  
39313139  
31343037 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030  
81890281  
8100C63C 4062B775 BC85E840 7A3220BF 78FE8C29 25012113 563A808F  
37F387BF  
CE7D58E6 A5CCAACC 25B7DC8D 956D7A2D F31BEB36 7406C5FB  
3AE82042 10CF68BE  
C5C710EF 1DDC5D75 F58E8CEE 2F695BBE 85AC5F88 42020E24  
A7132599 BC974991  
A5ADDBDA D36B5B2C 5D0EDB18 04B27BE5 1E8B107B E70670D5  
21FCA6A7 8926D3B9  
9E790203 010001A3 78307630 0F060355 1D130101 FF040530 030101FF  
30230603  
551D1104 1C301A82 18434559 5053412E 63657970 73612E75 74632E65  
64752E65  
63301F06 03551D23 04183016 8014077C A50DD6D8 04434CE9 67BEA0E5  
11DD8FC9  
6B0E301D 0603551D 0E041604 14077CA5 0DD6D804 434CE967 BEA0E511  
DD8FC96B  
0E300D06 092A8648 86F70D01 01040500 03818100 32B0FD3F 8B63C974  
74EECD53  
9622DE58 622B62FA 3C0ABA28 4850B916 ED398B4B 79222E24  
1FB5BD7E 0C1C78B2  
CF8DEB22 813844DD F141C4CD 32B6BC2E 3FA73693 E8A2FC40  
171CEF1C 187557D5

```
AD81255E D8385B77 4770DD94 E28B1440 39467F05 3D6E3425 72B36877
51810A13
```

```
2574A1D7 8BFEED08 FA796684 1DA4A241 AB83F3B9
```

```
quit
```

```
!
```

```
!
```

```
*** Nombre de usuario con privilegios de administracion
```

```
username CEYPSA privilege 15 view root password 0 *****
```

```
!
```

```
!
```

```
**** definición de los puertos a verificar según los protocolos
```

```
class-map type inspect match-all sdm-nat-http-1
```

```
match access-group 103
```

```
match protocol http
```

```
class-map type inspect match-all sdm-nat-smtp-1
```

```
match access-group 102
```

```
match protocol smtp
```

```
class-map type inspect match-any SDM_TELNET
```

```
match access-group name SDM_TELNET
```

```
class-map type inspect match-any SDM_HTTP
```

```
match access-group name SDM_HTTP
```

```
class-map type inspect match-any SDM_SHELL
```

```
match access-group name SDM_SHELL
```

```
class-map type inspect match-any SDM_SSH
```

```
match access-group name SDM_SSH
```

```
class-map type inspect match-any SDM_HTTPS
```

```
match access-group name SDM_HTTPS
```

```
class-map type inspect match-any sdm-mgmt-cls-0
```

```
match class-map SDM_TELNET
```

```
match class-map SDM_HTTP
match class-map SDM_SHELL
match class-map SDM_SSH
match class-map SDM_HTTPS
class-map type inspect match-any sdm-cls-insp-traffic
match protocol cuseeme
match protocol dns
match protocol ftp
match protocol h323
match protocol https
match protocol icmp
match protocol imap
match protocol pop3
match protocol netshow
match protocol shell
match protocol realmedia
match protocol rtsp
match protocol smtp extended
match protocol sql-net
match protocol streamworks
match protocol tftp
match protocol vdolive
match protocol tcp
match protocol udp
class-map type inspect match-all sdm-insp-traffic
match class-map sdm-cls-insp-traffic
class-map type inspect match-any remote-access
match protocol tcp
match protocol udp
match protocol icmp
class-map type inspect match-any sdm-cls-icmp-access
match protocol icmp
```

```
match protocol tcp
match protocol udp
class-map type inspect match-any sdm-service-sdm-inspect-1
match protocol https
match protocol http
match protocol msnmsgr
match protocol aol
match protocol ymsgr
class-map type inspect match-all sdm-cls-sdm-permit-1
match class-map remote-access
match access-group name access
class-map type inspect match-any sdm-dmz-protocols
match protocol http
match protocol pop3s
match protocol ftp
match protocol smtp
match protocol https
match protocol imaps
class-map type inspect match-all sdm-dmz-traffic
match access-group name dmz-traffic
match class-map sdm-dmz-protocols
class-map type inspect match-all sdm-mgmt-cls-sdm-permit-0
match class-map sdm-mgmt-cls-0
match access-group 106
class-map type inspect match-all sdm-icmp-access
match class-map sdm-cls-icmp-access
class-map type inspect match-any web
match protocol http
match protocol https
match protocol smtp
match protocol imap
match protocol imaps
```

```
match protocol imap3
match protocol pop3
match protocol pop3s
match protocol msnmsgr
class-map type inspect match-all sdm-invalid-src
  match access-group 101
  match class-map web
class-map type inspect match-all sdm-protocol-http
  match class-map sdm-service-sdm-inspect-1
!
!
```

\*\*\* establecimiento de políticas par a las diferentes zonas

```
policy-map type inspect sdm-permit-icmpreply
  class type inspect sdm-icmp-access
  inspect
class class-default
  pass
policy-map type inspect sdm-pol-NATOutsideToInside-1
  class type inspect sdm-nat-smtp-1
  inspect
  class type inspect sdm-nat-http-1
  inspect
class class-default
policy-map type inspect sdm-inspect
  class type inspect sdm-invalid-src
  inspect
  class type inspect sdm-insp-traffic
  inspect
  class type inspect sdm-protocol-http
  inspect
class class-default
```

```

policy-map type inspect sdm-permit
  class type inspect sdm-cls-sdm-permit-1
    inspect
  class type inspect sdm-mgmt-cls-sdm-permit-0
    inspect
  class class-default
policy-map type inspect sdm-permit-dmzservice
  class type inspect sdm-dmz-traffic
    inspect
  class type inspect sdm-nat-smtp-1
    inspect
  class type inspect sdm-nat-http-1
    inspect
  class class-default

```

!

\*\*\* definición de las zonas de seguridad

```

zone security dmz-zone
zone security out-zone
zone security in-zone
zone-pair security sdm-zp-self-out source self destination out-zone
  service-policy type inspect sdm-permit-icmpreply
zone-pair security sdm-zp-NATOutsideToInside-1 source out-zone destination in-
zo
ne
  service-policy type inspect sdm-pol-NATOutsideToInside-1
zone-pair security sdm-zp-out-dmz source out-zone destination dmz-zone
  service-policy type inspect sdm-permit-dmzservice
zone-pair security sdm-zp-out-self source out-zone destination self
  service-policy type inspect sdm-permit
zone-pair security sdm-zp-in-dmz source in-zone destination dmz-zone
  service-policy type inspect sdm-permit-dmzservice

```

```

zone-pair security sdm-zp-in-out source in-zone destination out-zone
service-policy type inspect sdm-inspect
!
!
!
!
!

```

\*\*\* Configuración de cada de una de las interfaces del Router , configuración de las Vlan

```

interface Null0
no ip unreachable
!
interface FastEthernet0/0
description DMZ$FW_DMZ$$ETH-LAN$
ip address 192.168.1.1 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp
ip nat inside
no ip virtual-reassembly
zone-member security dmz-zone
ip route-cache flow
duplex auto
speed auto
!
interface FastEthernet0/1
description WAN$FW_OUTSIDE$$ETH-LAN$
ip address 201.219.38.67 255.255.255.248
ip verify unicast reverse-path
no ip redirects
no ip unreachable

```

```
no ip proxy-arp
ip nat outside
no ip virtual-reassembly
zone-member security out-zone
ip route-cache flow
duplex half
speed 10
!
interface FastEthernet0/0/0
description Oficina
switchport access vlan 10
!
interface FastEthernet0/0/1
description Administracion
switchport access vlan 20
!
interface FastEthernet0/0/2
description Salas
switchport access vlan 30
!
interface FastEthernet0/0/3
description Wireless
switchport access vlan 40
!
interface Vlan1
ip address 10.100.100.1 255.255.255.252
no ip redirects
no ip unreachable
no ip proxy-arp
ip route-cache flow
!
interface Vlan10
```

```

description Oficina$FW_INSIDE$
ip address 10.10.10.1 255.255.255.0
ip access-group 107 in
no ip redirects
no ip unreachablees
no ip proxy-arp
ip nat inside
ip virtual-reassembly
rate-limit output 128000 64000 92000 conform-action transmit exceed-action
drop
zone-member security in-zone
ip route-cache flow
!
interface Vlan20
description Administracion$FW_INSIDE$
ip address 10.10.20.1 255.255.255.0
ip access-group 108 in
no ip redirects
no ip unreachablees
no ip proxy-arp
ip nat inside
ip virtual-reassembly
rate-limit output 64000 64000 64000 conform-action transmit exceed-action drop
zone-member security in-zone
ip route-cache flow
!
interface Vlan30
description Salas$FW_INSIDE$
ip address 10.10.30.1 255.255.255.0
no ip redirects
no ip unreachablees
no ip proxy-arp

```

```

ip nat inside
ip virtual-reassembly
rate-limit output 256000 64000 128000 conform-action transmit exceed-action
dro
p
zone-member security in-zone
ip route-cache flow
!
interface Vlan40
description Wireless$FW_INSIDE$
ip address 10.10.40.1 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp
ip nat inside
ip virtual-reassembly
rate-limit output 64000 32000 64000 conform-action transmit exceed-action drop
zone-member security in-zone
ip route-cache flor
!

*** parámetros para el ruteo
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1
ip route 0.0.0.0 0.0.0.0 201.219.38.65
!
!

*** parámetros de la configuración del NAT
ip http server
ip http access-class 1
ip http secure-server
ip nat inside source list 100 interface FastEthernet0/1 overload

```

```
ip nat inside source static tcp 192.168.1.2 25 201.219.38.66 25 extendable
ip nat inside source static tcp 192.168.1.2 80 201.219.38.66 80 extendable
!
```

\*\*\*\* Configuración de las políticas del NAT

```
ip access-list extended SDM_HTTP
 remark SDM_ACL Category=0
 permit tcp any any eq www
ip access-list extended SDM_HTTPS
 remark SDM_ACL Category=0
 permit tcp any any eq 443
ip access-list extended SDM_SHELL
 remark SDM_ACL Category=0
 permit tcp any any eq cmd
ip access-list extended SDM_SSH
 remark SDM_ACL Category=0
 permit tcp any any eq 22
ip access-list extended SDM_TELNET
 remark SDM_ACL Category=0
 permit tcp any any eq telnet
ip access-list extended access
 remark SDM_ACL Category=128
 permit ip any host 10.254.0.248
ip access-list extended dmz-traffic
 remark SDM_ACL Category=1
 permit ip any host 192.168.1.1
 permit ip any host 192.168.1.2
!
```

\*\*\* definición de las lista de control de acceso

```
access-list 1 remark Auto generated by SDM Management Access featurre
access-list 1 remark SDM_ACL Category=1
```

```
access-list 1 permit 10.10.20.0 0.0.0.255
access-list 1 permit 10.10.10.0 0.0.0.255
access-list 1 permit 201.219.38.0 0.0.0.255
access-list 100 remark SDM_ACL Category=128
access-list 100 permit ip host 255.255.255.255 any
access-list 100 permit ip 127.0.0.0 0.255.255.255 any
access-list 100 permit ip 10.10.50.0 0.0.0.255 any
access-list 100 permit ip 10.10.40.0 0.0.0.255 any
access-list 100 permit ip 10.10.30.0 0.0.0.255 any
access-list 100 permit ip 10.10.20.0 0.0.0.255 any
access-list 100 permit ip 10.10.10.0 0.0.0.255 any
access-list 100 permit ip 201.219.38.64 0.0.0.7 any
access-list 100 permit ip 192.168.1.0 0.0.0.255 any
access-list 101 remark SDM_ACL Category=128
access-list 101 permit ip host 255.255.255.255 any
access-list 101 permit ip 127.0.0.0 0.255.255.255 any
access-list 101 permit ip 10.10.20.0 0.0.0.255 any
access-list 101 permit ip 10.10.30.0 0.0.0.255 any
access-list 101 permit ip 10.254.0.0 0.0.0.255 any
access-list 101 permit ip 10.10.40.0 0.0.0.255 any
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
access-list 101 permit ip 10.10.10.0 0.0.0.255 any
access-list 102 remark SDM_ACL Category=0
access-list 102 permit ip any host 192.168.1.2
access-list 103 remark SDM_ACL Category=0
access-list 103 permit ip any host 192.168.1.2
access-list 104 remark Auto generated by SDM Management Access feature
access-list 104 remark SDM_ACL Category=1
access-list 104 permit tcp 201.219.38.0 0.0.0.255 host 201.219.38.67 eq telnet
access-list 104 permit tcp 201.219.38.0 0.0.0.255 host 201.219.38.67 eq 22
access-list 104 permit tcp 201.219.38.0 0.0.0.255 host 201.219.38.67 eq www
access-list 104 permit tcp 201.219.38.0 0.0.0.255 host 201.219.38.67 eq 443
```

```
access-list 104 permit tcp 201.219.38.0 0.0.0.255 host 201.219.38.67 eq cmd
access-list 104 deny tcp any host 201.219.38.67 eq telnet
access-list 104 deny tcp any host 201.219.38.67 eq 22
access-list 104 deny tcp any host 201.219.38.67 eq www
access-list 104 deny tcp any host 201.219.38.67 eq 443
access-list 104 deny tcp any host 201.219.38.67 eq cmd
access-list 104 deny udp any host 201.219.38.67 eq snmp
access-list 104 permit ip any any
access-list 105 remark Auto generated by SDM Management Access feature
access-list 105 remark SDM_ACL Category=1
access-list 105 permit ip 10.10.20.0 0.0.0.255 any
access-list 105 permit ip 10.10.10.0 0.0.0.255 any
access-list 105 permit ip 201.219.38.0 0.0.0.255 any
access-list 106 remark Auto generated by SDM Management Access feature
access-list 106 remark SDM_ACL Category=1
access-list 106 permit ip 201.219.38.0 0.0.0.255 host 10.254.0.248
access-list 107 remark Auto generated by SDM Management Access feature
access-list 107 remark SDM_ACL Category=1
access-list 107 permit tcp 10.10.10.0 0.0.0.255 host 10.10.10.1 eq telnet
access-list 107 permit tcp 10.10.10.0 0.0.0.255 host 10.10.10.1 eq 22
access-list 107 permit tcp 10.10.10.0 0.0.0.255 host 10.10.10.1 eq www
access-list 107 permit tcp 10.10.10.0 0.0.0.255 host 10.10.10.1 eq 443
access-list 107 permit tcp 10.10.10.0 0.0.0.255 host 10.10.10.1 eq cmd
access-list 107 deny tcp any host 10.10.10.1 eq telnet
access-list 107 deny tcp any host 10.10.10.1 eq 22
access-list 107 deny tcp any host 10.10.10.1 eq www
access-list 107 deny tcp any host 10.10.10.1 eq 443
access-list 107 deny tcp any host 10.10.10.1 eq cmd
access-list 107 deny udp any host 10.10.10.1 eq snmp
access-list 107 permit ip any any
access-list 108 remark Auto generated by SDM Management Access feature
access-list 108 remark SDM_ACL Category=1
```

```

access-list 108 permit tcp 10.10.20.0 0.0.0.255 host 10.10.20.1 eq telnet
access-list 108 permit tcp 10.10.20.0 0.0.0.255 host 10.10.20.1 eq 22
access-list 108 permit tcp 10.10.20.0 0.0.0.255 host 10.10.20.1 eq www
access-list 108 permit tcp 10.10.20.0 0.0.0.255 host 10.10.20.1 eq 443
access-list 108 permit tcp 10.10.20.0 0.0.0.255 host 10.10.20.1 eq cmd
access-list 108 deny tcp any host 10.10.20.1 eq telnet
access-list 108 deny tcp any host 10.10.20.1 eq 22
access-list 108 deny tcp any host 10.10.20.1 eq www
access-list 108 deny tcp any host 10.10.20.1 eq 443
access-list 108 deny tcp any host 10.10.20.1 eq cmd
access-list 108 deny udp any host 10.10.20.1 eq snmp
access-list 108 permit ip any any
no cdp run
!
access-list 108 permit ip any any
no cdp run
!
!
!
!
control-plane
!
!
```

\*\*\* parámetros de seguridad para el acceso del Router

```

line con 0
line aux 0
line vty 0 4
access-class 105 in
exec-timeout 60 0
password *****
login
```

```
transport input telnet ssh
transport output telnet ssh
!
scheduler allocate 20000 1000
!
end
```

### 3.11 Conclusiones

- Todo el desarrollo ha sido elaborado teniendo en cuenta las necesidades observadas en coordinación el Administrador de la Red de Datos CEYPSA, la Dirección de Servicios Informáticos de la UTC y la compañía proveedora del soporte operativo de la Red del CEYPSA como es la empresa READYNET.
- La Configuración del Router sirve para optimizar la Administración de la Red de Datos del CEYPSA, evitando que los usuarios externos e internos utilicen el Internet como plataforma de acceso en forma inadecuada a la información operativa de nuestra institución
- Mediante la Configuración del Router se encamina el acceso a paginas que son necesarias habilitando solo los parámetros requeridos por el Administrador garantizando su operatividad.
- Los Routers tienen la capacidad para discriminar entre paquetes y restringirlos en sus puertos con base en criterios específicos de protocolo se va a proceder con tácticas de filtración de paquetes, así como la toma de decisiones basándose en tablas de datos y reglas, por medio de filtros, a fin de que sólo datos de una cierta dirección puedan pasar a través del Router de la Universidad.
- La presente Tesis de Grado contribuye con la seguridad de la información de la Red de Datos del CEYPSA, al controlar el tráfico que pasa directamente entre las redes proporcionando un mecanismo poderoso de direccionamiento y por lo tanto restringir servicios que pueden poner en peligro la seguridad de la información de la Universidad Técnica de Cotopaxi.
- En el desarrollo de este proyecto, se dan los pasos necesarios para establecer un nivel óptimo de seguridad en la red de datos de la Universidad, que enseñará al personal encargado a tomar este tema como uno de los puntos claves para el buen funcionamiento del sistema.
- La Administración de la Red de Datos se conceptualiza como: Optimización y Seguridad

### 3.12 Recomendaciones

- Las universidades como centros de investigación siempre deben de buscar tecnologías que permitan dar el mismo o mejor servicio a menor costo, así como explotar el conocimiento y la iniciativa de los alumnos, bajo la acertada guía de los docentes.
- Implementar en la Carrera de Ingeniería en Sistemas Informáticos y Computacionales una asignatura teórica como práctica en que se estudie el desarrollo de Seguridades en Redes las que significan la solución a problemas de la tecnología sociedad abaratando costos y dando un buen servicio.
- Realizar continuamente una evaluación a la solución implementada para la UTC con la finalidad de tener en cuenta los estándares y tecnologías nuevas y de mayor penetración, lo cual nos ahorrará dinero, tiempo y problemas de incompatibilidad y nos brindará una comunicación rápida, eficiente y transparente.
- Utilizar el Manual de Usuario, en caso de sufrir un daño en el software del Router CISCO serie 2811 del CEYPSA.
- Se recomienda realizar un estudio con la finalidad de implementar Routers, en las otras Sedes de la UTC (Edificio Matriz y Sede la Maná), ya que todas sin excepción poseen servicio de Internet de banda ancha, y a través de estos servicios se maneja información operativa de importancia para todos los integrantes de la UTC

### **3.13 BIBLIOGRAFIA**

#### **3.13.1|BIBLIOGRAFÍA CITADA**

- Biblioteca de Consulta Microsoft® Encarta. (2006) [CD]. Microsoft Corporation, 2005, (Interactiva).
- Diccionario de la Real Academia de la Lengua, (2006), Ediciones Cultural, Madrid- España.
- Gustavo Rueda, (2000), Redes y Comunicaciones, comercializadora editorial y sistemas Ltda., Bogotá- Colombia.
- Julian Espinosa, (2002), Técnico en Telecomunicaciones, Cultural , S.A., Madrid-España.
- M Schwartz, (2000). Cableado de redes, tercera edición, paraninfo.
- Randall K .Nichols, (2003). Seguridad para comunicaciones, Msgraw-Hill.
- STALLINGS WILLIAM, (2000), Comunicaciones y Redes de Computadoras, Pearson Educación, 2000.

#### **3.13.2 BIBLIOGRAFIA CONSULTADA**

- DOUGLAS COMER, TCP/IP, Vol 1, Prentice Hall, 1996.
- FRENZEL LOUIS E., Sistemas Electrónicos de Comunicación, Alfaomega, 2003.
- JESÚS GARCÍA TOMÁS, Alta velocidad y calidad de servicios en redes IP, Alfaomega, 2002.
- TOMASI WAYNE, Sistemas de Comunicaciones Electronicas, Prentice Hall, 1996.
- UYLESS BLACK, Redes de Computadoras, Alfaomega, 1995.

### 3.13.3 BIBLIOGRAFIA VIRTUAL

- <http://www.abcdatos.com/tutoriales/tutorial/11311.html>
- <http://ciscopress.com>, Cisco Systems Inc. CCNA 1,2,3,4.
- [www.cientec.com/analisis/puente.asp](http://www.cientec.com/analisis/puente.asp)
- [http://es.geocities.com/yeiko\\_6/index.htm?/yeiko\\_6/router Cisco.htm](http://es.geocities.com/yeiko_6/index.htm?/yeiko_6/router%20Cisco.htm)
- [www.hispasec.com](http://www.hispasec.com)
- [www.ilustrados.com/publicaciones/EpypkElZlkSbFkXUCq.php](http://www.ilustrados.com/publicaciones/EpypkElZlkSbFkXUCq.php)
- [www.lpsi.eui.upm.es/SInformatica/SInformatica.htm](http://www.lpsi.eui.upm.es/SInformatica/SInformatica.htm)
- [www.monografias.com/trabajos/hackers/hackers.shtml](http://www.monografias.com/trabajos/hackers/hackers.shtml)
- [www.mslatam.com/latam/technet/cso/Html-ES/home.asp](http://www.mslatam.com/latam/technet/cso/Html-ES/home.asp)
- [www.monografias.com/trabajos/tesisgrado/tesisgrado.shtml](http://www.monografias.com/trabajos/tesisgrado/tesisgrado.shtml)
- [www.osmosislatina.com/conectividad/router Ciscos.htm](http://www.osmosislatina.com/conectividad/router%20Ciscos.htm)
- [www.pdvsa.com/lexico/tesis/tesis.htm](http://www.pdvsa.com/lexico/tesis/tesis.htm)
- <http://www.solont.com/>
- [http://www.htmlweb.net/redes/router Ciscos/router Ciscos\\_2.html](http://www.htmlweb.net/redes/router%20Ciscos/router%20Ciscos_2.html)
- Simulador BOSON NET SIMM FOR CCNP



Latacunga, a 20 abril del 2008

## CERTIFICADO

En calidad de Encargada del Área de Inglés de la Unidad Educativa San José "La Salle", tengo a bien:

### CERTIFICAR

Que he revisado y corregido el ABSTRACT de la Tesis de Grado denominada "**CONFIGURACIÓN DE UN ROUTER PARA OPTIMIZAR LA ADMINISTRACIÓN DE LA RED DE DATOS DEL CENTRO DE EXPERIMENTACIÓN Y PRODUCCIÓN SALACHE DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI**" de autoría de los señores Paúl C. Castellano M. y José W. Vaca A.

Es todo cuanto puedo certificar en honor de la verdad, pudiendo los interesados hacer uso del presente Certificado dentro de los fines legales que ellos creyeran conveniente.

Atentamente.

*Lic. Digna Castellano M.*

ENGLISH TEACHER  
DATE *[Signature]*

Lcda. Digna M. Castellano MSc.

ENCARGADA DEL AREA DE INGLES "LA SALLE"



# UNIVERSIDAD TECNICA DE COTOPAXI

## CENTRO DE COMPUTO UNIVERSITARIO

LATACUNGA - ECUADOR

### ACTA DE ENTREGA RECEPCION DEL EQUIPO CISCO 2811 ENTRE LOS SEÑORES: JOSE VACA, ESTUDIANTE DE LA CARRERA DE CIENCIAS DE LA INGENIERIA Y APLICADAS, Y EL ING ADRIAN MENA OPERADOR DE COMPUTADORES CEYPSA, al 12 de febrero del 2008.

En la ciudad de Latacunga, a los dose días del mes de febrero del dos mil ocho en el local donde funciona el Centro de Cómputo de la Universidad Técnica de Cotopaxi CEYPSA, se constituyen por una parte el Sr. José Vaca estudiante de la Carrera de Ciencia de la Ingeniería y Aplicadas, y po otra el Ing. Adrián Mena Operador de Computadores, con el objeto de proceder a la entrega recepción de un Equipo Cisco 2811, el mismo que sera ocupado en la Administración de la Red Informática del CEYPSA, equipo que se entrega luego de concluir la Tesis de Grado desarrollada por el Sr. José Vaca y el Sr. Paúl Castellano.

Para el efecto y la intervención de las personas antes mencionadas, se procede a la entrega recepción de lo siguiente: -----

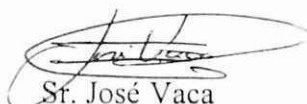
Número	Código Serie	Descripción	Estado
1	FTXC927A2RK	Router Cisco 2811	Nuevo

Además, el equipo tiene las siguientes claves de acceso:

Modo Gráfico:            Usuario: fmoya            Password: rdyec1791  
Modo Exec:                Password: utc2007

Para constancia de lo actuado en fe de conformidad, suscriben el presente documento en dos ejemplares del mismo tenor y efecto, quienes intervienen en la presente diligencia.

ENTREGUE CONFORME



Sr. José Vaca  
ESTUDIANTE UTC.

RECIBI CONFORME



Ing. Adrian Mena  
Operador de Computadores CEYPSA- UTC



# UNIVERSIDAD TÉCNICA DE COTOPAXI

## SALAS DE INTERNET CEYPSA

### LATACUNGA ECUADOR

---

Salache, a 12 de febrero del 2008

## CERTIFICADO

En calidad de Administrador de la Red de Datos del CEYPSA de la Universidad Técnica de Cotopaxi, tengo a bien

### CERTIFICAR

Que los señores **Paúl César Castellano Moreno** con C.I. 050198742-4 y **José Washintong Vaca Armendariz** con C.I. 050175133-3 Egresados de la Universidad Técnica de Cotopaxi Especialidad de Ingeniería en Sistemas Informáticos y Computacionales han concluido con la **“CONFIGURACION DE UN ROUTER PARA OPTIMIZAR LA ADMINISTRACION DE LA RED DE DATOS DEL CENTRO DE EXPERIMENTACION Y PRODUCCION SALACHE DE LA UNIVERSIDAD TECNICA DE COTOPAXI”**.

Trabajo en el cual se realizaron las configuraciones y una serie de pruebas; sujetándose a todas las especificaciones técnicas solicitadas.

Es todo cuanto puedo certificar en honor a la verdad, pudiendo los interesados hacer uso del presente certificado dentro de los fines legales que ellos creyeran conveniente.

Atentamente.

Ing. MSc. Adrián Mena Rojas  
**ADMINISTRADOR RED CEYPSA**



UNIVERSIDAD TÉCNICA DE COTOPAXI  
CARRERA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

LATACUNGA ECUADOR

---

# **GUÍA DE USUARIO**

# **ROUTER CISCO 2811**



## ÍNDICE

	Página
Portada .....	1
Índice .....	2
Introducción .....	4
Contenido .....	4
Objetivos del Manual de Usuario .....	4
Usuarios del Router Cisco 2811 .....	4
Uso del Módulo .....	4
Visión General del Documento .....	5
Capítulo I .....	6
Introducción .....	6
Requerimientos para instalación de SDM de cisco .....	6
Principio de un Router .....	6
La familia IOS .....	6
Tipos de release .....	6
Numeración T .....	7
Numeración S .....	7
Numeración XR.....	7
Partes del Router .....	7
Ciclo de Vida .....	7
Router Cisco 2811 .....	8
Especificaciones .....	8
Conectividad .....	10
Instalación de SDM de Cisco .....	11
Instalación de JAVA .....	14
Modos de acceso al Router .....	16
Modo línea de comando – EXEC .....	17
Modos de usuario y privilegiado .....	18
Comandos más importantes del modo usuario .....	18
Modo EXEC Usuario .....	18
Modo EXEC Privilegiado .....	20
Modo de configuración global .....	21
Submodo de configuración de interfaz .....	23
Submodo de configuración de línea .....	24
Comandos de edición y otros .....	24
Casos prácticos .....	24
Modo Gráfico SDM .....	27
Información del Router del Ceypsa .....	30
Pantalla de información general .....	30
Opción de configuración .....	32
Configuración de las interfaces .....	33
Configuración del Firewall .....	33
Enrutamiento .....	34



NAT .....	35
Tareas adicionales .....	35
Capítulo II .....	38
Configuración del Router cisco 2811 .....	38
Introducción .....	38
De la red de datos y laboratorios informáticos del Ceypsa .....	38
Funciones del encargado de la red de datos y laboratorios .....	38
Diseño de la red del Ceypsa .....	39
Configuración del ancho de banda para las diferentes VLAN.....	40
Configuración del Router 2811 del Ceypsa .....	40



## INTRODUCCION

Este documento es una Especificación de Requisitos Software (ERS) para el Router CISCO 2811 del Centro de Experimentación Salache de la Universidad Técnica de Cotopaxi, se constituye en el medio oficial de proveer documentación técnica a los usuarios del Router CISCO 2811 del CEYPSA; y resalta sus características más significativas. También describe las instrucciones de diseño que permiten determinar los requisitos específicos.

Desafortunadamente, las intrusiones en redes por parte de usuarios externos e internos se han convertido en un suceso habitual, lo que significa que las organizaciones deben instalar alguna protección contra las mismas. Un Router Cisco cuesta dinero y supone un impedimento para el flujo de tráfico. Por lo tanto, debe asegurarse de que el Router Cisco esté configurado para ser tan rentable y eficaz como sea posible.

## CONTENIDO

Este módulo contiene información, instrucciones así como los procedimientos pertinentes a todos los trabajos de operación mantenimiento y modificación de configuraciones del Router CISCO 2811 del CEYPSA. Todo su contenido ha sido elaborado teniendo en cuenta las necesidades observadas en la Red de Datos del CEYPSA. La información precisada en este Manual de Usuario se halla establecida en función de varios programas de muestreo aplicados por el grupo postulante, basados en publicaciones emitidas por la Compañía Cisco Systems así como en varias organizaciones gubernamentales y privadas que basan el flujo de sus Redes en Routers Cisco.

## OBJETIVO DEL MANUAL DE USUARIO

- Definir de manera clara y precisa todas las funcionalidades y restricciones del Router Cisco 2811 del CEYPSA que se desee configurar.

## USUARIOS DEL ROUTER CISCO 2811

El documento va dirigido a los usuarios autorizados por la Dirección de Servicios Informáticos de la Universidad Técnica de Cotopaxi y a los proveedores de del Servicio de Internet siendo en este caso la empresa READYNET. Este documento será el canal de comunicación entre las partes implicadas, tomando parte en su confección miembros de cada parte.

## USO DEL MÓDULO

Antes de comenzar a dar uso operativo a este módulo, el lector debería poseer algunos conocimientos generales sobre las instrucciones de los Routers Cisco. También resulta útil ponerse al corriente a cerca del origen, uso, aplicación y cambios de las instrucciones de diseño que se presentan en este módulo, teniendo en cuenta consideraciones importantes



como el crecimiento de la red y el cambio de configuraciones en el Router. Este módulo define también las distintas clases de instrucciones de rediseño, el responsable de manipular estos cambios debe poder seleccionar la clase que se ajuste mejor a sus necesidades. A partir de los conocimientos y la terminología técnica proporcionados en este módulo, podrá analizar con los usuarios del Router Cisco los cambios que pueden ofrecerle y evaluar si se adecúan o no a sus necesidades.

## VISIÓN GENERAL DEL DOCUMENTO

Más allá de la experiencia o conocimientos que cada uno de nosotros tenga en la administración y configuración Redes Informáticas, al momento de tener que realizar o modificar la configuración de una interfaz, es importante que tengamos en cuenta algunas claves, que son comunes a todas las interfaces de los dispositivos CISCO. Ante todo, todos los comandos relacionados con la configuración de algún aspecto de las interfaces, se ejecutan en el modo configuración de consola.

Con el fin de conocer las principales funciones que realiza un Router, así como los datos asociados, los factores, restricciones, supuestos y dependencias que afectan al desarrollo de la Configuración del Router Cisco 2811 del CEYPSA, se ha llegado a la conclusión que es necesario dividir al Manual de Usuario en dos capítulos:

- CAPITULO I**            **GENERALIDADES DE LOS ROUTERS CISCO**  
En este Capítulo se proporciona una visión general de las perspectivas del Router así como de las especificaciones generales de los Router Cisco, maneras de configurar los Router Cisco, Detalle de las instrucciones más utilizadas
- CAPITULO II**        **CONFIGURACIÓN DEL ROUTER CISCO 2811 DEL CEYPSA**  
En este Capítulo se da un a descripción específica de la Configuración del Router Cisco 2811 del Centro de Experimentación y Producción Salcache de la UTC.

Este documento ha sido objeto de revisiones por las partes implicadas, especialmente por los usuarios finales, que se recogieron por medio de sucesivas versiones del documento, hasta alcanzar su aprobación.



## CAPITULO I

### GENERALIDADES DE LOS ROUTERS CISCO

#### INTRODUCCION

CISCO SYSTEMS es una compañía californiana dedicada a las redes, en sus catálogos se incluyen Routers, Switches, Cortafuegos, etc. CISCO vende tanto el Hardware como Software incluyendo varias versiones de IOS (Sistemas Operativos) por lo que el 70% del tráfico de Internet circula por dispositivos CISCO

Una investigación no puede ser exitosa sin una serie de pruebas operativas con parámetros que cumplan con los requerimientos, para ello se necesita muchas destrezas técnicas; por lo que el desarrollo del presente trabajo se basa en dos aspectos de mucha importancia:

- La utilización de los sistemas de configuración del propio Router (interfaz Exec), que es el sistema operativo propiamente dicho
- SDM que permite la configuración en modo gráfico del equipo.

#### REQUERIMIENTOS PARA INSTALACION DE SDM DE CISCO

##### HARDWARE

Mínimo un equipo Pentium 4 ó Superior  
Mínimo 128 Mb. en RAM  
Mínimo 100 Libres en espacio de Disco Duro

##### SOFTWARE

Sistema operativo Windows XP Professional, 2003 Server Stantad Edition o 2000 Professional con Service Pack 4.  
Windows 2000 Advanced Server NO está soportado.  
Navegador de Internet Firefox 1.0.6+, Internet Explorer 5.5+ o Netscape 7.1 o 7.2.  
Habilitar el uso de ventanas emergentes.  
Sun Java Runtime Environment (JRE) versiones.  
Software de Instalación SDM Ver 2.4.1 de Cisco

#### PRINCIPIOS DE UN ROUTER

##### LA FAMILIA IOS

Hay muchas versiones de IOS cuya nomenclatura está estandarizada

##### TIPO DE RELEASE:

**Mainline:** Versión de IOS más estable. No se añaden funcionalidades sobre y sólo se realizan actualizaciones por bugs



<b>T: Technology.</b>	Modifica una mainline por una demanda de una actualización por bug o una nueva funcionalidad. El hardware no está incluido.
<b>S: Service Provider.</b>	Optimizada para los clientes proveedores de Servicios.
<b>SB: Funcionalidad</b>	Funcionalidad y hardware de banda ancha de equipos de gama media para el borde de red (routers)
<b>SX:</b>	Equipos Ethernet-LAN de altas prestaciones para core de red (switchs)
<b>SE, SG:</b>	Equipos Ethernet-LAN de rango medio-bajo (switchs)
<b>SR:</b>	Equipos Ethernet-LAN de altas prestaciones para borde de red (routers)
<b>E: Enterprise.</b>	Optimizada para entornos empresariales.
<b>B: Broadband.</b>	Optimizada para banda ancha
<b>XR:</b>	Optimizada para el core de red y con capacidad de direccionar terabits de tráfico.

#### NUMERACIÓN T:

La versión principal actual del IOS para el Router Cisco 2811 del CEYPSA es la 12

12.4(7a) Es una versión mainline 12.4 release 7a

12.4(9)T3 Es la tercera versión T basada en la mainline 12.4(9)

#### NUMERACIÓN S:

12.2(28)SB1: Primera revisión de la 12.2(28) de SB (para routers medianos)

#### NUMERACIÓN XR:

No tiene más que números: 12.3.1

### PARTES DEL ROUTER

Esta sección contiene un Repertorio total de todos los componentes Aplicables del Router Cisco 2811, entre estos tenemos:

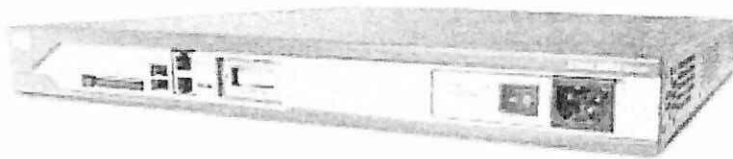
<b>RAM/DRAM:</b>	Guarda tablas de enrutamiento, ARP, valores temporales, ...
<b>NVRAM:</b>	Almacena la configuración
<b>FLASH:</b>	Almacena el IOS arrancable
<b>ROM:</b>	Guarda el bootstrap. Para actualizarla hay que cambiar el chip
<b>INTERFACES:</b>	Conexiones de red

### CICLO DE VIDA

<b>FCS:</b>	First Customer Shipment. A disposición del cliente
<b>EoS:</b>	End of Sale. Se deja de vender el producto, pero se siguen sacando actualizaciones.
<b>EoE:</b>	End of Engineering. No se sacan más actualizaciones pero se sigue dando soporte.
<b>EoL:</b>	End of Life. Únicamente se da soporte en caso de migración a una versión más actual.



## ROUTER CISCO 2811



### ESPECIFICACIONES

<b>GENERAL</b>	
Tipo de dispositivo	Encaminador
Factor de forma	Externo - modular - IU
Anchura	43.8 cm
Profundidad	41.7 cm
Altura	4.5 cm
Peso	6.4 kg

<b>MEMORIA</b>	
Memoria RAM	256 MB (instalados) / 760 MB (máx.)
Memoria Flash	64 MB (instalados) / 256 MB (máx.)

<b>CONEXIÓN DE REDES</b>	
Tecnología de conectividad	Cableado
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Red / Protocolo de transporte	IPSec
Protocolo de gestión remota	SNMP 3
Indicadores de estado	Actividad de enlace, alimentación
Características	Protección firewall, cifrado del hardware, alimentación mediante Ethernet (PoE), VPN, soporte de MPLS, filtrado de URL
Cumplimiento de normas	IEEE 802.3af



<b>EXPANSION / CONECTIVIDAD</b>	
Total ranuras de expansión (libres)	4 ( 4 ) x HWIC   2 ( 2 ) x AIM   1 ( 1 ) x NME   2 ( 2 ) x PVDM   2 memoria   1 Tarjeta CompactFlash
Interfaces	6 x red - Ethernet 10Base-T/100Base-TX - RJ-45   2 x USB   1 x gestión - consola   1 x red - aux

<b>ALIMENTACION</b>	
Dispositivo de alimentación	Fuente de alimentación – interna
Voltaje necesario	CA 120/230 V ( 47 - 63 Hz )

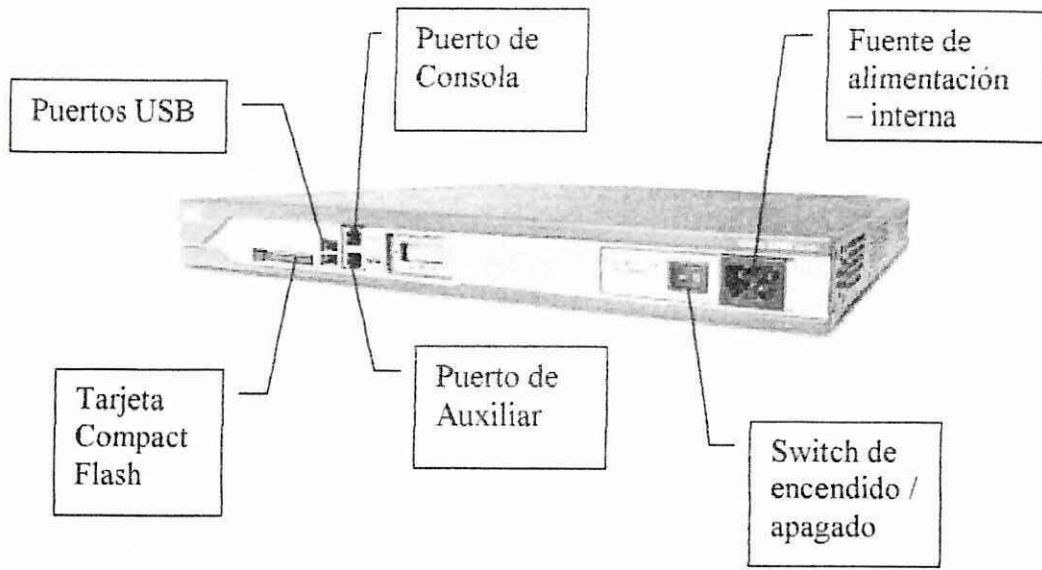
<b>SOFTWARE</b>	
OS proporcionado	Cisco IOS 12.3(8)T
Sistema operativo requerido	Microsoft Windows 98 Second Edition

<b>PARAMETROS DE ENTORNO</b>	
Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	40 °C
Ambito de humedad de funcionamiento	5 - 95%

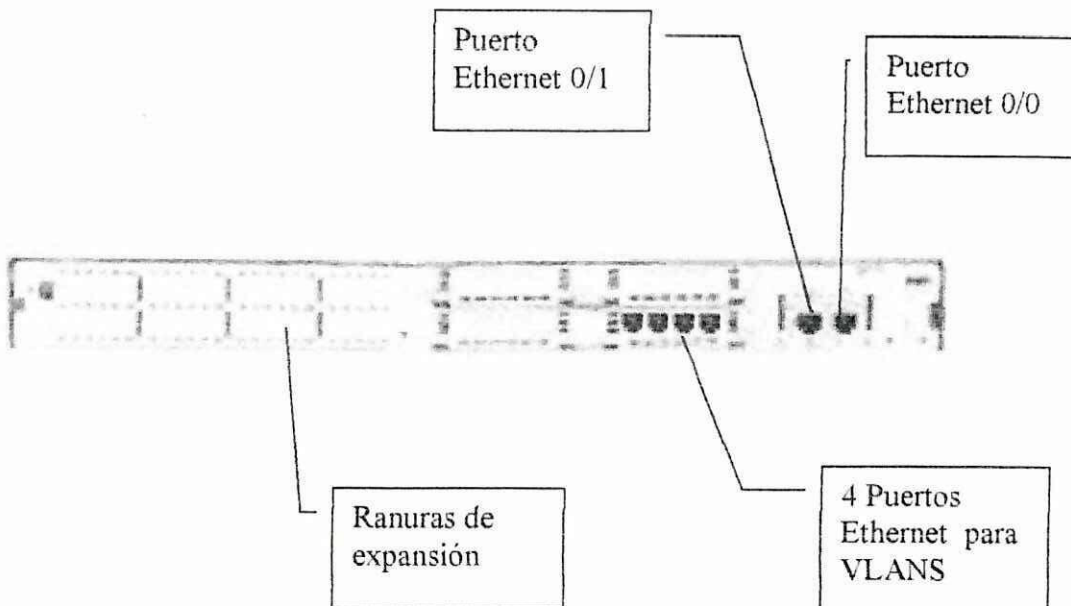


## CONECTIVIDAD

### Parte Frontal



### Parte Posterior





## INSTALACION DE SDM DE CISCO

SDM es el anagrama abreviado de Cisco Router and Security Device Manager. Una herramienta de management basada en web desarrollada por Cisco. No es simplemente una interfaz web. Es una herramienta java accesible a través de un web browser.

Esta herramienta soporta un rango extremadamente amplio de routers Cisco IOS: desde los routers de la familia 8xx, hasta los de la serie 73xx. En la actualidad se entrega preinstalado en todos los routers de servicios integrados nuevos de las series 850, 870, 1800, 2800 y 3800.

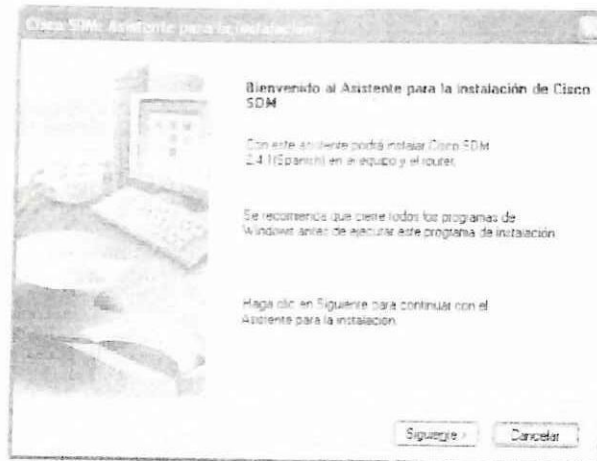
Es importante mencionar que el proceso de instalación del software de SDM se ha desarrollado como soporte para el usuario ya que este sistema ya se encuentra instalado en el Router Cisco 2811 del Ceypsa y no se deberá realizar dicha instalación en este equipo.

A continuación se detalla el proceso de instalación, el mismo que sigue los siguientes pasos:

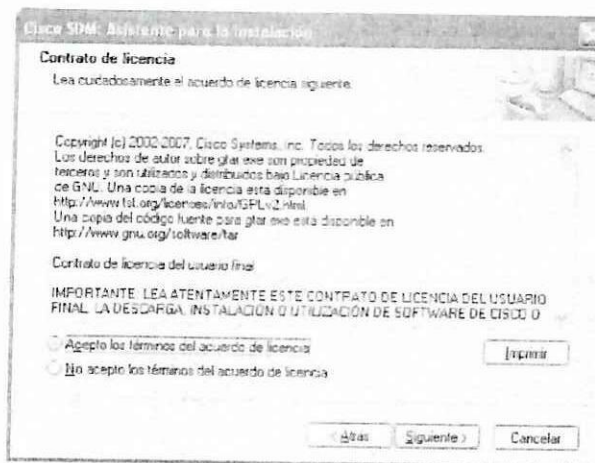
1. Ingresar a la carpeta de instalación de SDM, y ejecutar SETUP.EXE
2. Inicia el proceso de instalación, visualizando la siguiente información



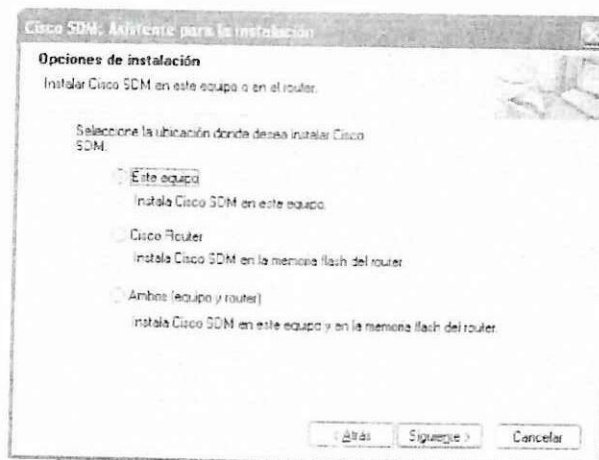
3. Se presenta la pantalla de bienvenida al software de instalación. Clic en el botón siguiente para continuar con la instalación



4. El siguiente punto es aceptar la licencia de uso del software y clic en siguiente. Cabe indicar que el software es gratuito distribuido por Cisco.



5. A continuación seleccionamos el tipo de instalación a realizar, las opciones son:



- **En este Equipo.-** Para instalar el software solamente en la estación de trabajo



- **Cisco Router.**- Para instalar el software solamente en la memoria del Router. En este caso el Router deberá estar conectado en red con la estación
- **Ambos.**- Para instalar el software tanto en la estación de trabajo como en el Router. En este caso el Router deberá estar conectado en red con la estación

Seleccionada la opción a instalar clic en siguiente

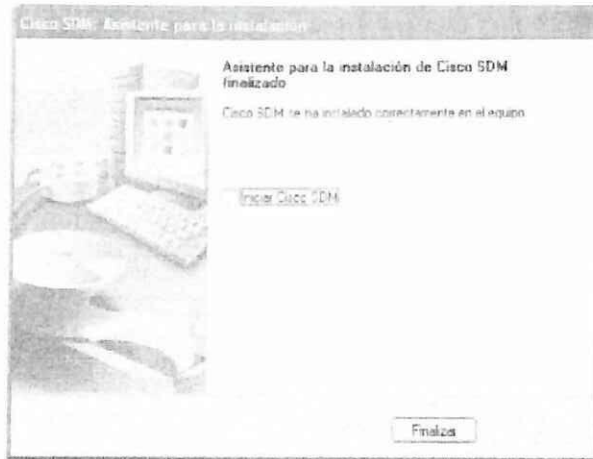
6. El siguiente paso es definir el directorio de la estación donde se instalará el software. Si no desea utilizar el que viene por defecto utilizar el botón **Examinar** para seleccionar una nueva ubicación. Definidos estos puntos clic en siguiente



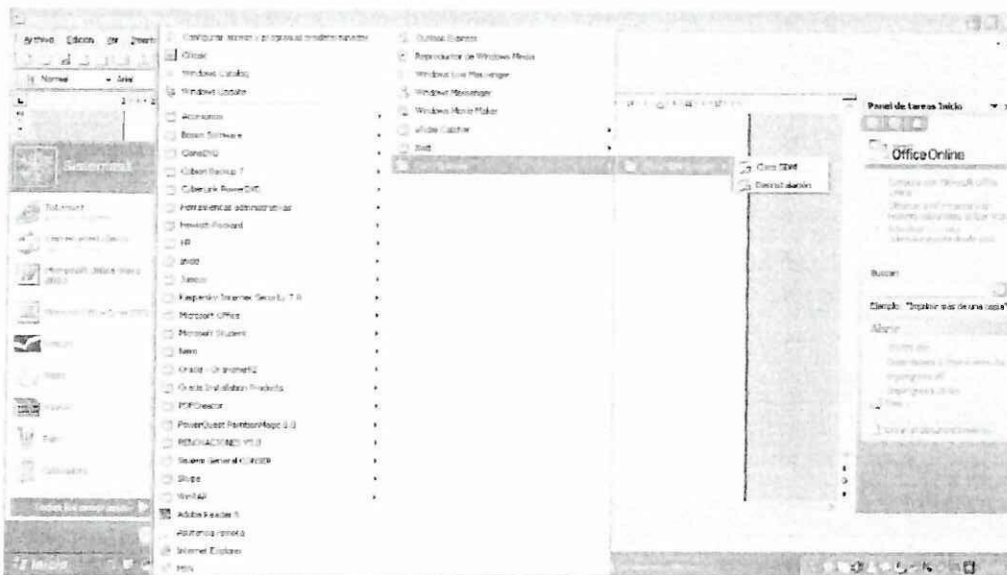
7. Se presentará la pantalla para iniciar la instalación, si desea realizar cambios utilice atrás caso contrario para iniciar la instalación clic en el botón Instalar.



8. El software se instala con las opciones señaladas anteriormente. Una vez concluido se presenta la siguiente pantalla.



9. Para ingresar al software se creará un acceso en Windows como se indica a continuación



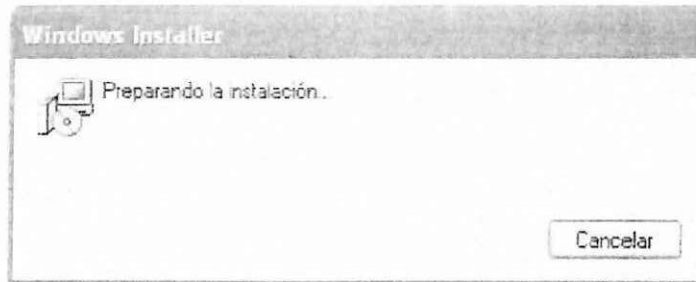
## INSTALACIÓN DE JAVA

Java es una plataforma virtual de software desarrollada por Sun Microsystems, de tal manera que los programas creados en ella puedan ejecutarse sin cambios en diferentes tipos de arquitecturas y dispositivos computacionales.

Es importante dejar establecido que sin este componente instalado en el equipo que tendrá acceso al Router en modo gráfico y por lo tanto no podrá utilizar el software de SDM.

El proceso de instalación es el siguiente:

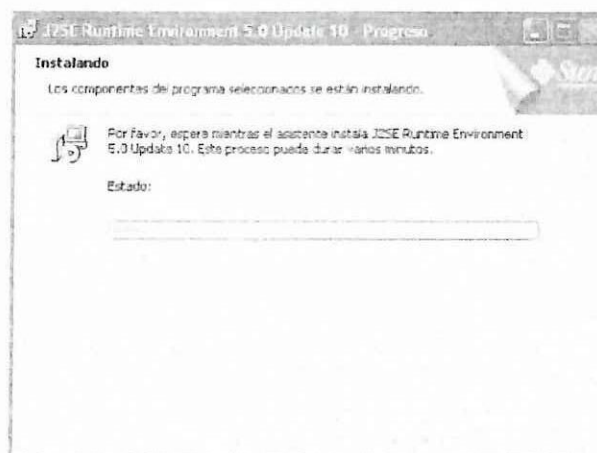
1. Ingresamos a la carpeta donde se encuentre disponible el instalador de Java y lo ejecutamos, el archivo es java\_runtime\_environment\_1\_5\_0\_10.exe
2. Se visualizará la pantalla que prepara la instalación



3. Completada la preparación de la instalación, se presenta la pantalla de aceptación de la licencia, hay que mencionar que es software de libre distribución; debemos seleccionar el tipo de instalación que en nuestro caso es Instalación Típica, y clic en Aceptar >

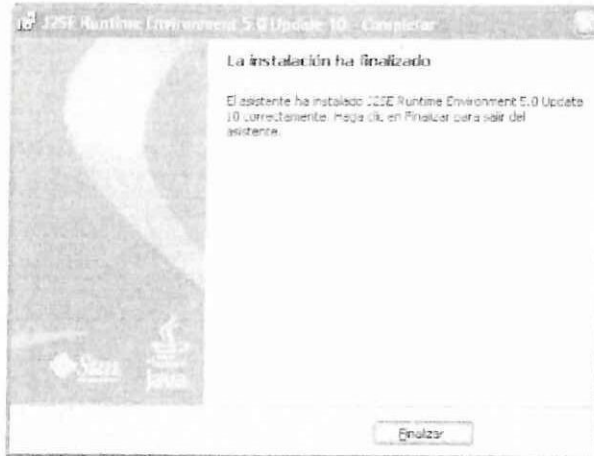


4. Inicia el proceso de instalación del software en el equipo





5. Luego del proceso de instalación se presenta la pantalla indicando el fin del proceso



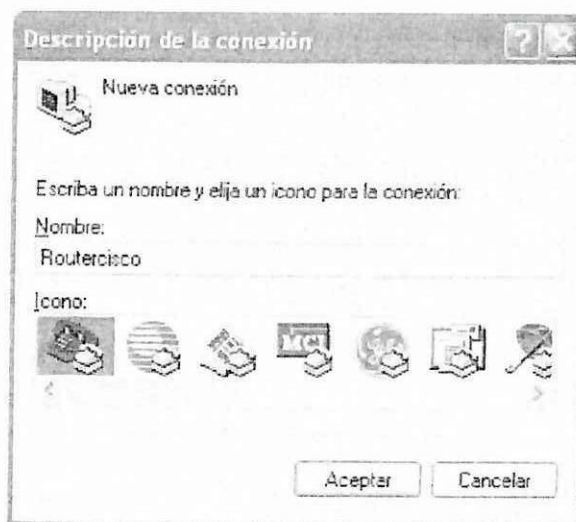
## MODOS DE ACCESO AL ROUTER

### MODO LÍNEA DE COMANDO - EXEC

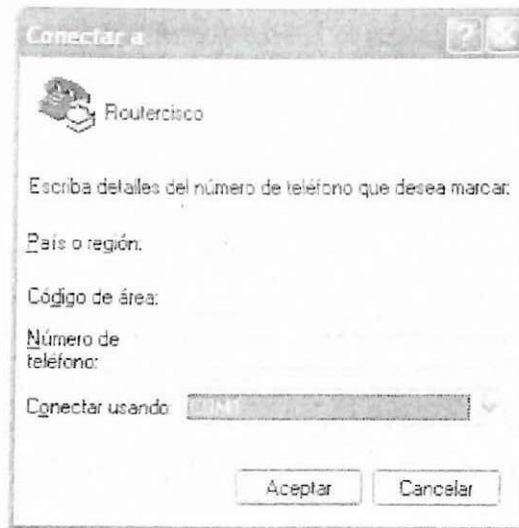
#### ACCESO AL IOS

Todos los routers tienen un puerto de consola, con cada router se incluye un cable azul para conectar al COM del ordenador y a la boca de consola del router, la consola del router se abre mediante el programa Hyperterminal que incluye Windows.

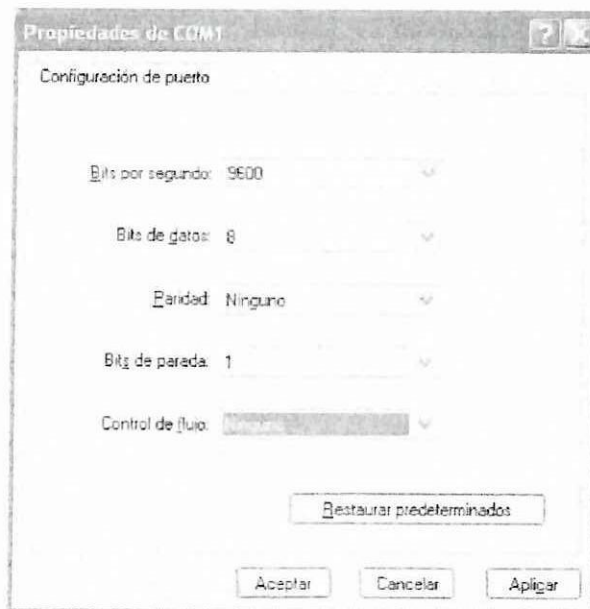
1. Una vez activado Hyperterminal definimos el nombre de la conexión



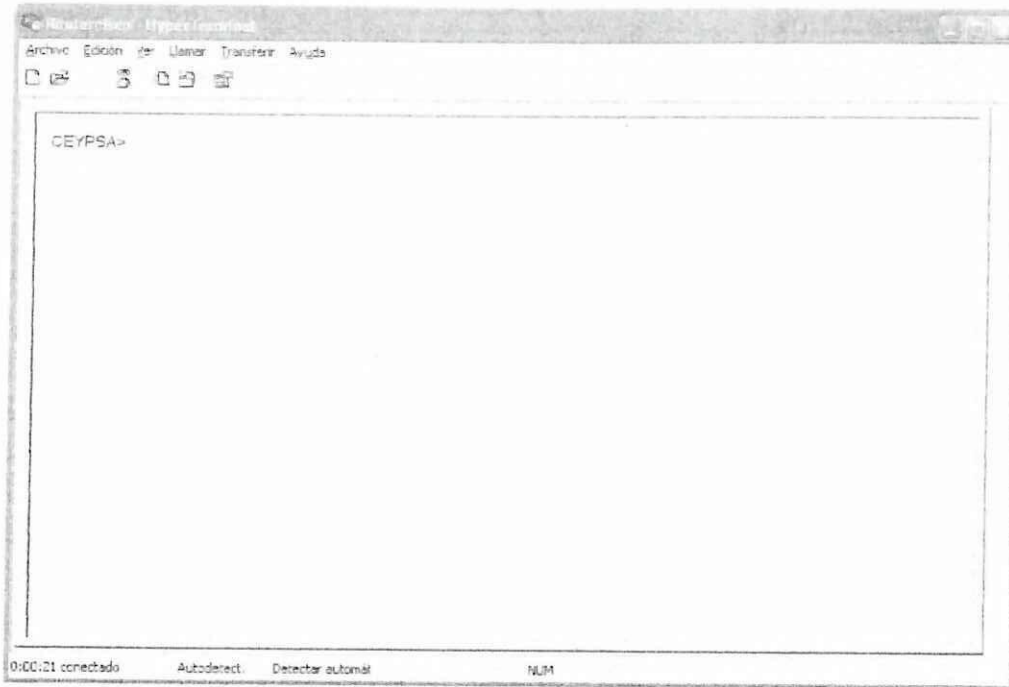
2. Se define el puerto a utilizar, en este caso COM1



3. Se define los siguientes parámetros



4. Presionando <<Enter>> se dispone de acceso al Router



Se puede trabajar en dos modos que son:

**Modo Usuario:** Sólo permite chequear el estado del modem, no se permiten cambios de configuración

**Modo Privilegiado:** Permite cambiar la configuración

Consideraciones:

- Una vez lograda la conexión entre el PC y el Router, para pasar al modo privilegiado, el comando es **“enable”**
- Para pedir ayuda sobre los comandos, sólo hay que teclear **“?”**
- IOS reconoce los comandos con sólo escribir unas letras. ¿Cuántas? Las suficientes como para que no haya ambigüedad en los comandos  
Ej: configure terminal = conf t  
Ej: enable = ena
- Es posible pulsar las teclas del cursor de arriba y abajo para navegar por el histórico de comandos introducidos (también sirve Ctrl-p y Ctrl-n)

## COMANDOS MÁS IMPORTANTES DEL MODO DE USUARIO

### MODO EXEC USUARIO

Comando	Descripción
connect { <i>dirección_ip</i>   <i>nombre</i> }	Permite conectarse remotamente a un host
disconnect <i>conexión</i>	Desconecta una sesión telnet establecida desde el router



enable	Ingresa al modo EXEC Privilegiado
logout	Sale del modo EXEC
ping { <i>dirección_ip</i>   <i>nombre</i> }	Envía una petición de eco para diagnosticar la conectividad básica de red
resume <i>conexión</i>	Resume una sesión telnet interrumpida con la secuencia CTRL+SHIFT+6 y X
show cdp	Muestra el intervalo entre publicaciones CDP, tiempo de validez y versión de la publicación
show cdp entry [*  <i>nombre_dispositivo</i> ] [ <i>protocol</i>   <i>version</i> ]	Muestra información acerca de un dispositivo vecino registrado en una tabla CDP
show cdp interfaces [ <i>tipo número</i> ]	Muestra información acerca de las interfaces en las que CDP está habilitado
show cdp neighbors [ <i>tipo número</i> ] [ <i>detail</i> ]	Muestra los resultados del proceso de descubrimiento de CDP
show clock	Muestra la hora y fecha del router
show history	Muestra el historial de comandos ingresados
show hosts	Muestra una lista en caché de los nombres de host y direcciones
show ip interface brief	Muestra un breve resumen de la información y del estado de una dirección IP
show ip rip database	Muestra el contenido de la base de datos privada de RIP
show ip route [ <i>dirección</i> ] [ <i>protocolo</i> ]	Muestra el contenido de la tabla de enrutamiento IP. El parámetro <i>dirección</i> permite acotar la información que se desea visualizar, exclusivamente a la dirección ingresada. El parámetro <i>protocolo</i> permite indicar la fuente de aprendizaje de las rutas que se desean visualizar, como por ejemplo <i>rip</i> , <i>igrp</i> , <i>static</i> y <i>connected</i>
show sessions	Muestra las conexiones Telnet establecidas en el router
show version	Muestra información sobre el Cisco IOS y la plataforma
telnet { <i>dirección_ip</i>   <i>nombre</i> }	Permite conectarse remotamente a un host
terminal editing	Reactiva las funciones de edición avanzada
terminal history size <i>número líneas</i>	Establece el tamaño del buffer del historial de comandos
terminal no editing	Deshabilita las funciones de edición avanzada
traceroute <i>dirección_ip</i>	Muestra la ruta tomada por los paquetes hacia un destino



### MODO EXEC PRIVILEGIADO

Comando	Descripción
clear cdp counters	Restaura los contadores de tráfico CDP a cero
clear cdp table	Elimina la tabla CDP de información de los vecinos
clear counters	Despeja los contadores de las interfaces
configure memory	Carga información de configuración de la NVRAM
configure terminal	Configura la terminal manualmente desde la terminal de consola
copy flash tftp	Copia la imagen del sistema desde la memoria Flash a un servidor TFTP
copy running-config startup-config	Guarda la configuración activa en la NVRAM
copy running-config tftp	Almacena la configuración activa en un servidor TFTP
copy tftp flash	Descarga una nueva imagen desde un servidor TFTP en la memoria Flash
copy tftp running-config	Carga la información de configuración desde un servidor TFTP
debug cdp adjacency	Muestra información recibida de vecinos CDP
debug cdp events	Muestra información sobre eventos CDP
debug cdp ip	Muestra información CDP específica de IP
debug cdp packets	Muestra información relacionada a los paquetes CDP
debug ip igrp events	Muestra todos los eventos IGRP que se están enviando y recibiendo en el router.
debug ip igrp transactions	Muestra las actualizaciones IGRP que se están enviando y recibiendo en el router
debug ip rip	Muestra información sobre las actualizaciones de enrutamiento RIP mientras el router las envía y recibe
debug ip rip [events]	Muestra las actualizaciones de enrutamiento RIP a medida que se las envía y recibe
disable	Salte del modo EXEC Privilegiado hacia el modo EXEC Usuario
erase flash	Borra el contenido de la memoria Flash
erase startup-config	Borra el contenido de la NVRAM
no debug all	Desactiva todas las depuraciones activadas en el dispositivo
reload	Reinicia el router
setup	Entra a la facilidad de Diálogo de configuración inicial
show access-lists [Nro_ACL][Nom-bre_ACL]	Muestra el contenido de todas las ACL en el router. Para ver una lista específica, agregue el nombre o número de ACL como opción a este comando



show arp	Muestra la asignación de direcciones IP a MAC a Interfaz del router
show cdp traffic	Muestra los contadores CDP, incluyendo el número de paquetes enviados y recibidos, y los errores de checksum
show controllers serial [número]	Muestra información importante como que tipo de cable se encuentra conectado
show debugging	Muestra información acerca de los tipos de depuraciones que están habilitados
show flash	Muestra la disposición y contenido de la memoria Flash
show interfaces [tipo número]	Muestra estadísticas para la/las interfaces indicadas
show ip interface [tipo número]	Muestra los parámetros de estado y globales asociados con una interfaz
show ip protocols [summary]	Muestra los parámetros y estado actual del proceso de protocolo de enrutamiento activo
show memory	Muestra estadísticas acerca de la memoria del router, incluyendo estadísticas de memoria disponible
show processes	Muestra información acerca de los procesos activos
show protocols	Muestra los protocolos de capa 3 configurados
show running-config	Muestra la configuración actual en la RAM
show sessions	Muestra las conexiones Telnet establecidas en el router
show stacks	Controla el uso de la pila de procesos y rutinas de interrupción y muestra la causa del último re arranque del sistema
show startup-config	Muestra la configuración que se ha guardado, que es el contenido de la NVRAM
terminal monitor	Si se utiliza una sesión por telnet para examinar el router, entonces, permite redirigir el resultado y los mensajes del sistema hacia a terminal remota
undebug all	Desactiva todas las depuraciones activadas en el dispositivo

### MODULO DE CONFIGURACIÓN GLOBAL

Comando	Descripción
access-list <i>Nro_ACL</i> {permit deny} <i>Origen</i>	Crea o agrega una sentencia de condición a la ACL que permitirá o denegará los paquetes que llegan desde un <i>Origen</i> . Este último parámetro puede ser una dirección IP más una máscara wildcard, la palabra host más una dirección IP o el wildcard any
access-list <i>Nro_ACL</i> {permit deny} <i>Proto Origen</i>	Crea o agrega una sentencia de condición a la ACL que permitirá o denegará los paquetes que lleguen



<i>Destino</i> [ <i>Operador Nro puerto</i> ] [established][echo  echo-reply]	desde un <i>Origen</i> y vayan hacia un <i>Destino</i> . <i>Proto</i> identifica el protocolo a verificar. <i>Origen</i> y <i>Destino</i> pueden ser una dirección IP más una máscara wildcard, la palabra host más una dirección IP o el wildcard any. <i>Operador</i> puede ser lt (menor que), gt (mayor que), eq (igual a) o neq (distinto a). <i>Nro puerto</i> indica el puerto TCP o UDP. El parámetro established permite el paso de tráfico cuando hay una sesión establecida. En el caso del protocolo ICMP se puede utilizar echo o echo-reply.
Banner motd #mensaje del día#	Configura un cartel con un mensaje del día. Ej: banner motd #Bienvenido#
boot system flash [nombre imagen IOS]	Especifica que el router cargue el IOS desde la Flash Ej: boot system flash c2500-IOS
boot system rom	Especifica que el router cargue el IOS desde la ROM
boot system tftp nombre_imagen IOS dir IP_server tftp	Especifica que el router cargue el IOS desde un servidor TFTP. Ej: boot system tftp c2500-IOS 24.232.150.1
cdp run	Habilita CDP globalmente en el router
clock set hh:mm:ss mes día año	Modificar la fecha y hora del router. Ej: clock set 12:31:00 July 12 2004
config-register valor registro configuración	Cambia los valores del registro de configuración. Ej: config-register 0x2142
enable password contraseña	Establece una contraseña local para controlar el acceso a los diversos niveles de privilegio. Ej: enable password class
enable secret contraseña	Especifica una capa de seguridad adicional mediante el comando enable password. Ej: enable secret class
hostname nombre	Modifica el nombre del router. Ej: hostname Lab_A
interface tipo número	Configura un tipo de interfaz y entra al modo de configuración de interfaz. Ej: interface ethernet 0
ip access-list { □tandard extended } Nombre	Permite crear una ACL nombrada. Se debe indicar el tipo. Este comando ingresa al router al submodo de configuración que puede reconocerse por el prompt Router(config-ext-nacl)#
ip classless	Permite que el router no tome en cuenta los límites con definición de clases de las redes en su tabla de enrutamiento y simplemente transmita hacia la ruta por defecto
ip default-network dirección_red	Establece una ruta por defecto. Ej: ip default-network 210.32.45.0
ip domain-lookup	Habilita la conversión de nombre a dirección en el router
ip host nombre_host dir_ip1 ....	Crea una entrada de nombre a dirección estática en el



<i>Dir_ip8</i>	archivo de configuración del router. Ej: ip host Lab A 192.168.5.1 210.110.11.1
ip http server	Permite que el router actúe como servidor Web http limitado
ip name-server <i>dir_ip1</i> .... <i>Dirip6</i>	Especifica las direcciones de hasta seis servidores de nombres para su uso para la resolución de nombres y direcciones.
Ip route <i>dirección_red máscara</i> <i>dir_ip_salto</i> [ <i>distancia administrativa</i> ]	Establece rutas estáticas. Ej: ip route 210.42.3.0 255.255.255.0 211.1.2.1
line <i>tipo número</i>	Identifica una línea específica para la configuración e inicia el modo de reunión de comandos de configuración. Ej: line console 0 ó line vty 0 4
router <i>protocolo_de_enrutamiento</i> [ <i>nro_AS</i> ]	Inicia un proceso de enrutamiento definiendo en primer lugar un protocolo de enrutamiento IP. Ej: router rip ó router igrp 120
service password-encryption	Habilita la función de cifrado de la contraseña

### SUBMODO DE CONFIGURACIÓN DE INTERFAZ

Comando	Descripción
bandwidth <i>Kbps</i>	Establece un valor de ancho de banda para una interfaz. Ej: bandwidth 64
cdp enable	Habilita Cisco Discovery Protocol en una interfaz
cdp holdtime <i>segundos</i>	Especifica el tiempo de espera antes de ser enviada la siguiente actualización CDP
cdp timer <i>segundos</i>	Especifica la frecuencia con que son enviadas actualizaciones CDP
clock rate <i>velocidad</i>	Configura la velocidad de reloj para las conexiones de hardware en interfaces seriales, como módulos de interfaz de red y procesadores de interfaz a una velocidad de bits aceptable. Ej: clock rate 56000
description <i>descripción</i>	Agrega una descripción a la interfaz. Ej: description Conectada a Internet
ip access-group <i>Nro_ACL</i> [in out]	Asigna la ACL indicada a la interfaz, ya sea para que verifique los paquetes entrantes (in) o los salientes (out)
ip address <i>dirección_ip</i> <i>máscara_red</i>	Asigna una dirección y una máscara de subred e inicia el procesamiento IP en una interfaz. Ej: ip address 192.168.52.1 255.255.255.0
no ip route-cache	Para <b>deshabilitar el balanceo de carga por destino</b> , que esté habilitado por defecto
no ip split-horizon	Deshabilita el horizonte dividido en la interfaz, que por defecto se encuentra habilitado. Para volver habilitarlo utilíce el comando ip split-horizon



no shutdown	Reinicia una interfaz desactivada
shutdown	Inhabilita una interfaz

### SUBMODO DE CONFIGURACIÓN DE LINEA

Comando	Descripción
access-class <i>Nro_ACL</i> in	En las líneas VTY, asigna una lista de control de acceso a las conexiones establecidas via Telnet
login	Habilita la verificación de contraseña en el momento de la conexión.
password <i>contraseña</i>	Asigna la contraseña a ser solicitada en el momento de la conexión

### COMANDOS DE EDICIÓN y OTROS

Teclas / Comando	Descripción
Ctrl+A	Permite desplazarse al principio de la línea de comandos
Esc+B	Permite desplazarse una palabra hacia atrás
Ctrl+B (o Flecha Izquierda)	Permite desplazarse un carácter hacia atrás
Ctrl+E	Permite desplazarse hasta el final de la línea de comandos
Ctrl+F (o Flecha Derecha)	Permite desplazarse un carácter hacia delante
Ctrl+P (o Flecha Arriba)	Muestra el último comando ingresado
Ctrl+N (o Flecha Abajo)	Muestra el comando más reciente
<Tab> (tecla Tabulador)	Completa el comando ingresado parcialmente
Ctrl+Z (o end)	Estando en cualquier modo de configuración regresa al modo EXEC Privilegiado
Ctrl+C	Cancela la ejecución del <i>Dialogo de configuración inicial o Setup</i>
Ctrl+Shift+6	Permite interrumpir intentos de ping, traceroute y traducciones de nombres
exit	Estando en el modo de configuración global o cualquiera de sus submodos regresa al modo anterior. Estando en los modos EXEC Usuario o EXEC Privilegiado, cierra la sesión

### CASOS PRACTICOS

#### Configuración del Hostname

```
Router#configure terminal
Router(config)#hostname [ceypsa]
ceypsa (config)#Ctrl + z
ceypsa #
```



## Configuración de Password

### 1.- Enable Password

```
ceypsa#configure terminal
ceypsa(config)#enable password [password]
ceypsa(config)#Ctrl + z
ceypsa#
```

### 2.- Enable Secret

```
ceypsa#configure terminal
ceypsa(config)#enable secret [password]
ceypsa(config)#Ctrl + z
ceypsa#
```

### 3.- Terminal

```
ceypsa#configure terminal
ceypsa(config)#line vty 0 4
ceypsa(config-line)#login
ceypsa(config-line)#password [password]
ceypsa(config-line)#Ctrl + z
ceypsa#
```

### 4.- Consola

```
ceypsa#configure terminal
ceypsa(config)#line console 0
ceypsa(config-line)#login
ceypsa(config-line)#password [password]
ceypsa(config-line)#Ctrl + z
ceypsa#
```

### 5.- Auxiliar

```
ceypsa#configure terminal
ceypsa(config)#line auxiliary 0
ceypsa(config-line)#login
ceypsa(config-line)#password [password]
ceypsa(config-line)#Ctrl + z
ceypsa#
```

### 6.- Configuración de la descripción de las Interfaces

```
ceypsa#configure terminal
ceypsa(config)#interface [interface]
ceypsa(config-if)#description [descripción]
ceypsa(config-if)#Ctrl + z
ceypsa#
```

### 7.- Configuración del Registro de Configuración

```
ceypsa#configure terminal
```



```
ceypsa(config)config-register [registro]
ceypsa(config)#Ctrl + z
ceypsa#
```

#### 8.- Configuración de las Direcciones de las Interfaces

```
ceypsa#configure terminal
ceypsa(config)#interface [interface]
ceypsa(config-if)#ip address [dirección] [máscara]
ceypsa(config-if)#no shutdown
ceypsa(config-if)#Ctrl + z
ceypsa#
```

#### 9.- Configuración del Protocolo

```
ceypsa#configure terminal
ceypsa(config)#router rip
ceypsa(config-router)#Ctrl.+z
ceypsa#
```

#### 10.- Configuración de Rutas Estáticas

```
ceypsa#configure terminal
ceypsa(config)#ip router ip [red_origen] [máscara_destino] [ip_interface_destino]
ceypsa(config)#Ctrl.+z
ceypsa#
```

### Comandos ACL estándar

Paso 1 Definir la ACL

```
ceypsa(config)# access-list [access-list-number] {permit | deny} {test-conditions}
```

Paso2: Aplicar la ACL a una interface

```
ceypsa(config-if)# {protocol} access-group [access-list-number]
```

### Comandos any

```
ceypsa(config)# access-list 1 permit 0.0.0.0 255.255.255.255
```

cualquier IP máscara wildcard

Se puede usar esto:

```
ceypsa(config)# access-list 1 permit any
```

### Comando host

```
ceypsa(config)# access-list 1 permit 192.168.1.2 0.0.0.0
```

dirección IP máscara wildcard

se puede usar esto:

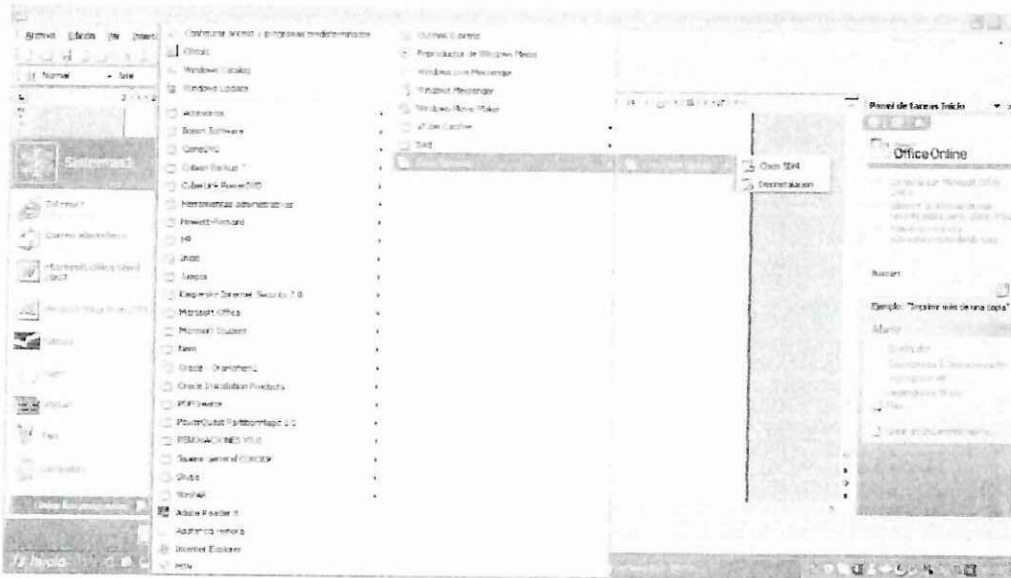
```
ceypsa(config)# access-list 1 permit host 192.168.1.2
```



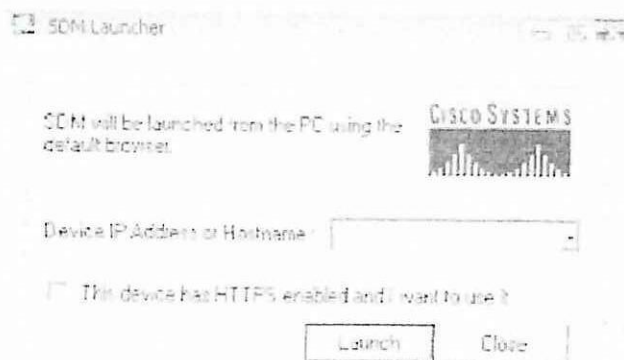
## MODO GRAFICO – SDM

El acceso a la configuración en modo gráfico mediante la utilización de SDM de Cisco se puede realizar de dos formas, las mismas que son:

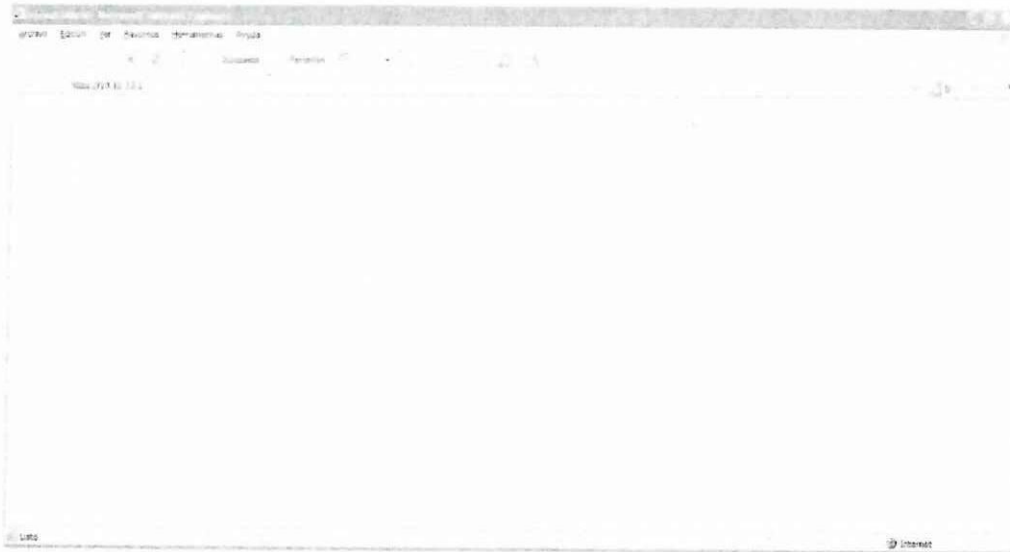
1. Ingresamos al software a través del acceso creado en la instalación



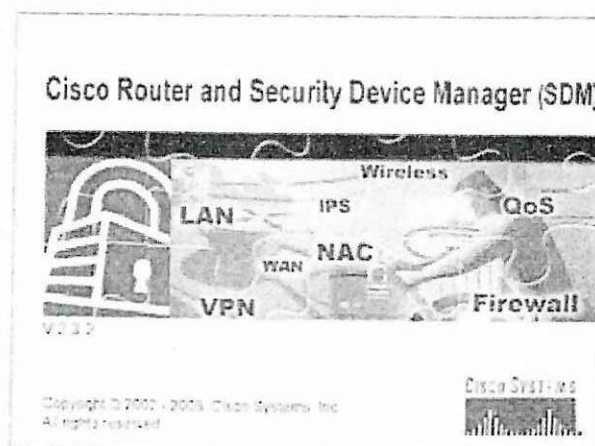
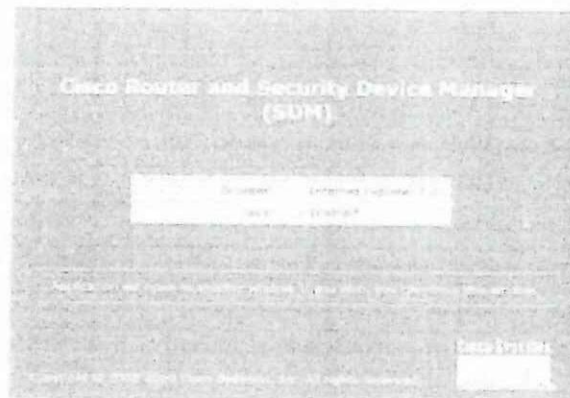
Se abrirá una ventana de diálogo requiriendo el ingreso de la dirección IP del dispositivo. Ingrese la IP del dispositivo e inmediatamente se abrirá una ventana del navegador de Internet para comenzar el proceso de carga.



2. Ingresar al web browse y digitar la dirección IP del Router, en el caso del Ceypsa la dirección IP es 10.10.10.1



En ambos casos se inicia el proceso de acceso a la información del Router mostrándose las siguientes pantallas





Como siguiente punto debemos ingresar el usuario y la clave para poder acceder a la configuración del equipo la veces que el sistema lo solicite.



## INFORMACIÓN DEL ROUTER DEL CEYPSA

### PANTALLA DE INFORMACIÓN GENERAL



#### 1. Menú de opciones

**Inicio.-** Permite visualizar la pantalla general de estadísticas del Router

**Configurar.-** Ingresa al modo de configuración del Router, en la cual se puede realizar entre otras las siguientes tareas: Parámetros de cada de las interfaces Ethernet, serial, etc. Configurar el Firewall y Listas de Control de Acceso. Parámetros de la Red Privada Virtual. Seguimiento a través de la Auditoría de Seguridad. Configurar el Enrutamiento. Definir las características del Network Address Translation. Es un standard de Internet que le permite a una red local (LAN) usar un grupo de direcciones de IP para el tráfico (NAT). Determinar como se va a realizar la Prevención de Intrusiones.

**Monitor.-** Visualiza el a través de gráficas todo el funcionamiento actual del Router

**Actualizar.-** Refresca toda la información que se visualiza de acuerdo a lo que este realizando el Router

**Guardar.-** Permite almacenar los cambios realizados en los parámetros de configuración

**Búsqueda.-** Opciones para buscar opciones o parámetros específicos

**Ayuda.-** Activa el módulo de ayuda del software SDM

#### 2. Información estadística del Router



## OPCION DE CONFIGURACION

The screenshot shows the Cisco IOS configuration interface. At the top, there is a menu bar with 'Archivo', 'Editar', 'Ver', 'Herramientas', and 'Ayuda'. Below the menu bar, there are icons for 'Inicio', 'Configurar', 'Monitor', 'Actualizar', 'Guardar', 'Búsqueda', and 'Ayuda'. The main area is titled 'Tareas' and contains a sub-menu 'Editar interfaz / conexión'. Below this, there is a 'Lista de interfaces' section with a table of interfaces. A large number '2' is overlaid on the table header. Below the table, there is a 'Detalles de la interfaz FastEthernet0/0' section with a table of configuration parameters. A large number '3' is overlaid on the right side of the interface list, and a large number '4' is overlaid on the right side of the details table.

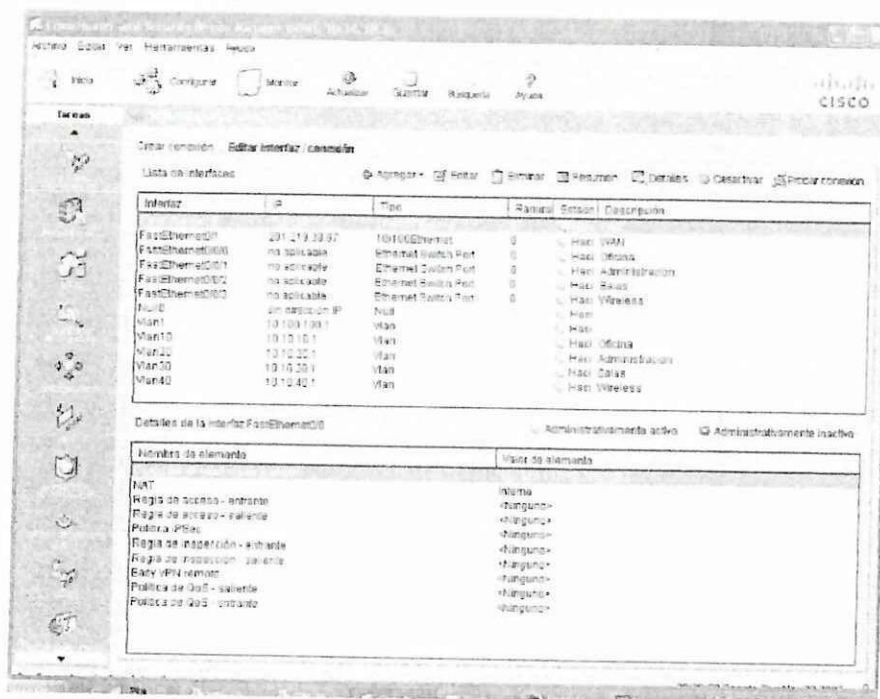
Interfaz	IP	Tipo	Ranura	Estado	Descripción
FastEthernet0/1	201.219.38.87	10/100 Ethernet	0		Haci WAN
FastEthernet0/0	no aplicable	Ethernet Switch Port	0		Haci Oficina
FastEthernet0/1	no aplicable	Ethernet Switch Port	0		Haci Administracion
FastEthernet0/2	no aplicable	Ethernet Switch Port	0		Haci Salas
FastEthernet0/3	no aplicable	Ethernet Switch Port	0		Haci Wireless
Null0	sin direccion IP	Null			Haci
Vlan1	10.100.100.1	Vlan			Haci
Vlan10	10.10.10.1	Vlan			Haci Oficina
Vlan20	10.10.20.1	Vlan			Haci Administracion
Vlan30	10.10.30.1	Vlan			Haci Salas
Vlan40	10.10.40.1	Vlan			Haci Wireless

Nombre de elemento	Valor de elemento
NAT	Interna
Regla de acceso - entrante	<Ninguno>
Regla de acceso - saliente	<Ninguno>
Política IPsec	<Ninguno>
Regla de inspección - entrante	<Ninguno>
Regla de inspección - saliente	<Ninguno>
Easy VPN remoto	<Ninguno>
Política de QoS - saliente	<Ninguno>
Política de QoS - entrante	<Ninguno>

1. Opciones de configuración del Router
2. Menú de trabajo, se tiene entre otras las opciones:
  - Agregar.**- Permite incrementar un elemento a la lista
  - Editar.**- Permite la modificación de los parámetros establecidos para cada elemento.
  - Eliminar.**- Quitar un elemento de la lista
  - Resumen.**- Visualiza los parámetros programados en el elemento seleccionado
  - Detalle.**- Visualiza en detalle los parámetros programados en el elemento seleccionado
  - Desconectar.**- Desactivar el elemento seleccionado
  - Probar conexión.**- Permite realizar un diagnóstico de funcionamiento del elemento seleccionado
3. Muestra la cabecera de la cada uno los elementos que consta el equipo
4. Despliega la información relacionada con el elemento seleccionado en la cabecera

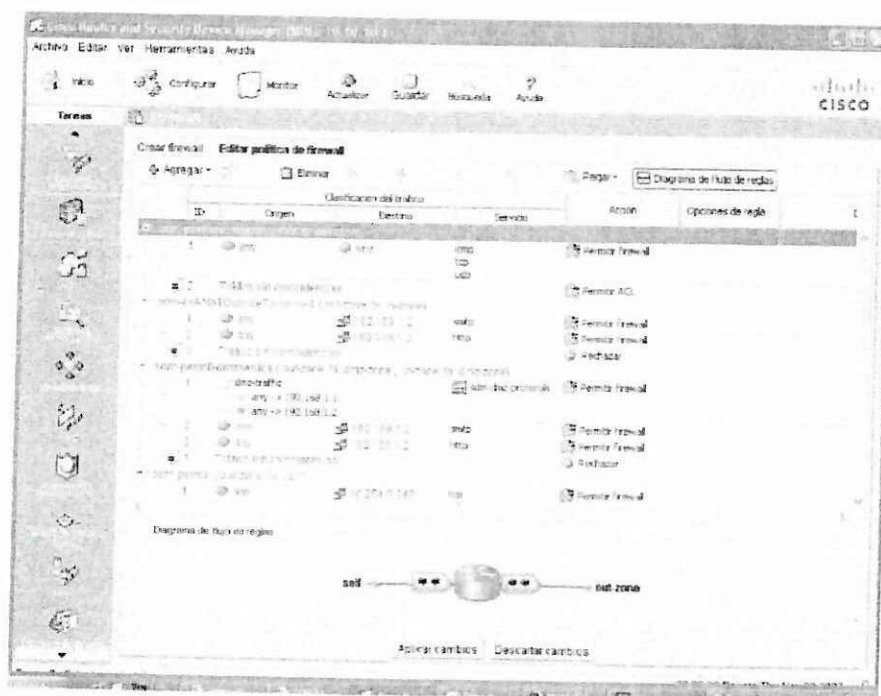


## CONFIGURACION DE LAS INTERFACES



Permite definir cada uno de los parámetros que constara cada una de las interfaces del Router, en este caso las Fast Ethernet 0/0 y 0/1. Las Fast Ethernet 0/0/0, 0/0/1, 0/0/2 y 0/0/3. Las VLAN para cada área

## CONFIGURACION DEL FIREWALL





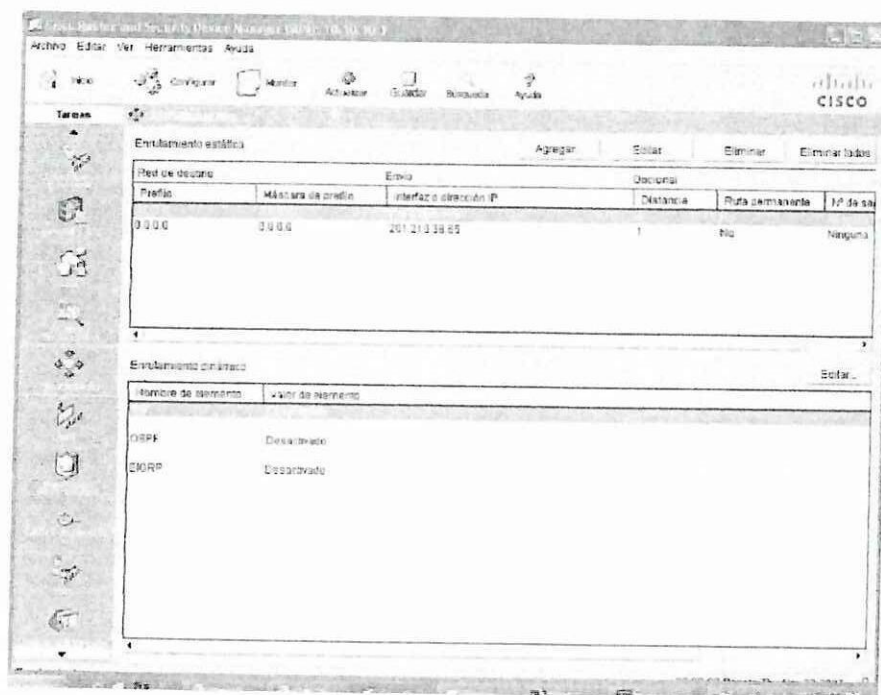
Se define cada una de las zonas de seguridad del equipo, las mismas que son:

1. Desde Internet hacia la red interna
2. Desde la red interna hacia Internet
3. Desde el Internet a la DMZ (Zona Desmilitarizada que es la zona física detrás de un servidor de seguridad de Internet y delante de un servidor de seguridad de segundo nivel que protege los sistemas y datos del servidor)
4. Desde la DMZ hacia el Internet

Determinado en cada una de las zonas los protocolos que se permiten utilizar y los que va a rechazar el servidor de seguridad

## ENRUTAMIENTO

Encaminamiento (o enrutamiento) Se trata de la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad. Dado que se trata de encontrar la mejor ruta posible, lo primero será definir que se entiende por mejor ruta y en consecuencia cual es la métrica que se debe utilizar para medirla



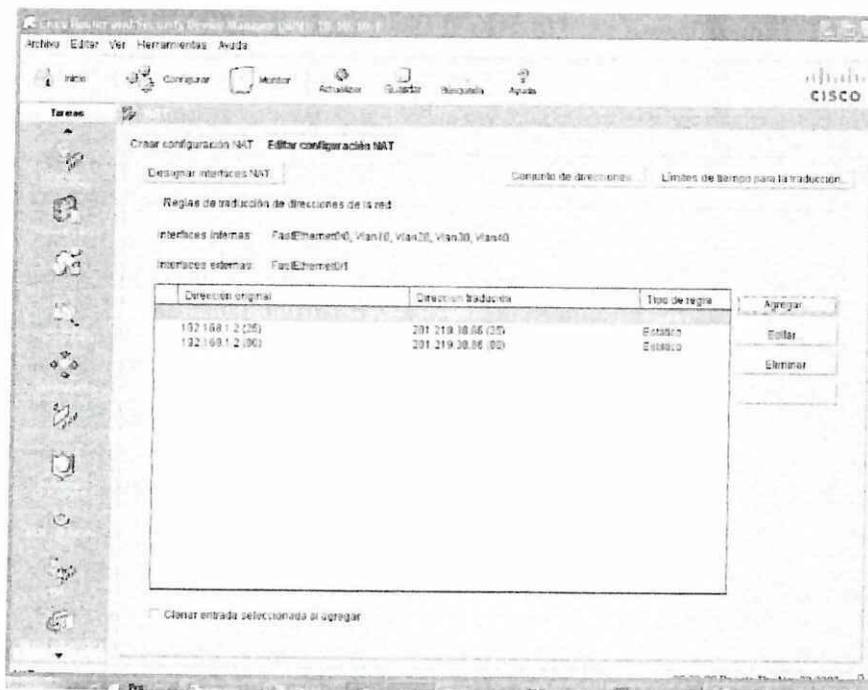
El enrutamiento permite establecer que interfaz del Router será utilizada para la conexión al equipo del proveedor de Internet, en nuestro caso la interfaz utilizada es la FastEthernet0/1 que apunta a la dirección 201.219.38.65 del equipo del proveedor.



## NAT

(Network Address Translation - Traducción de Dirección de Red) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

Este mecanismo en el caso del Router del Ceypsa esta definido de la siguiente manera:

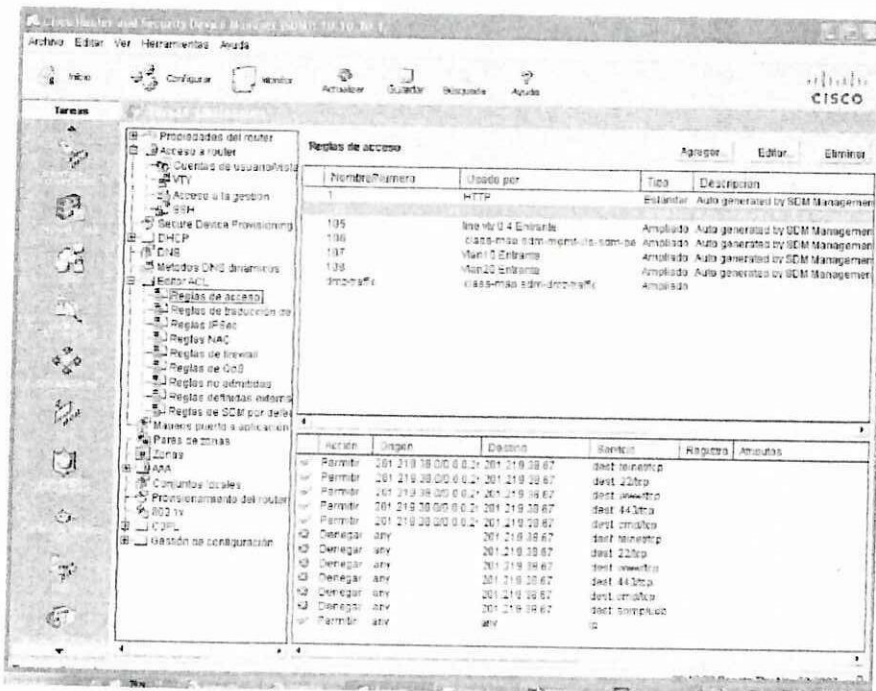
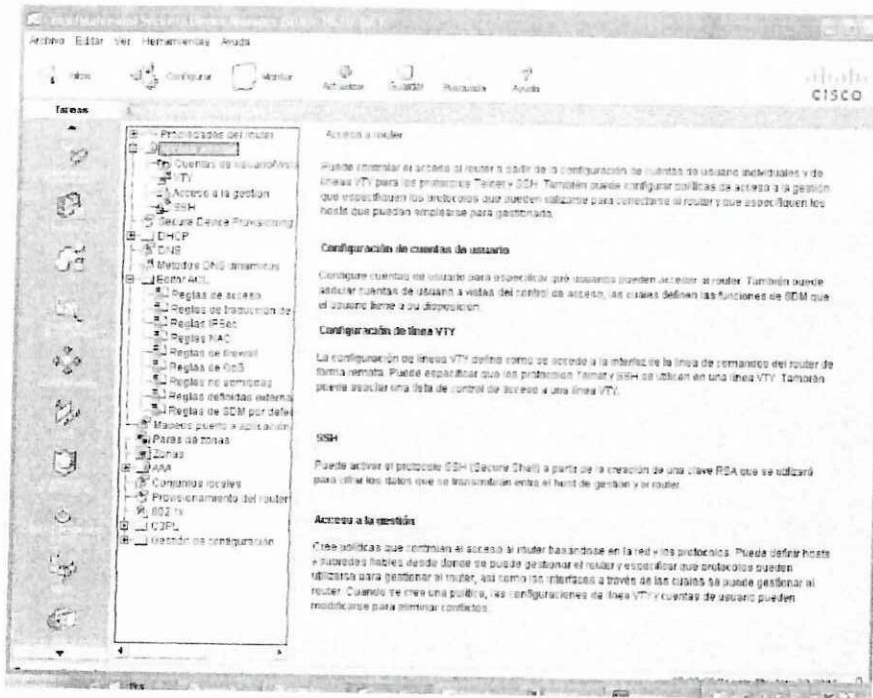


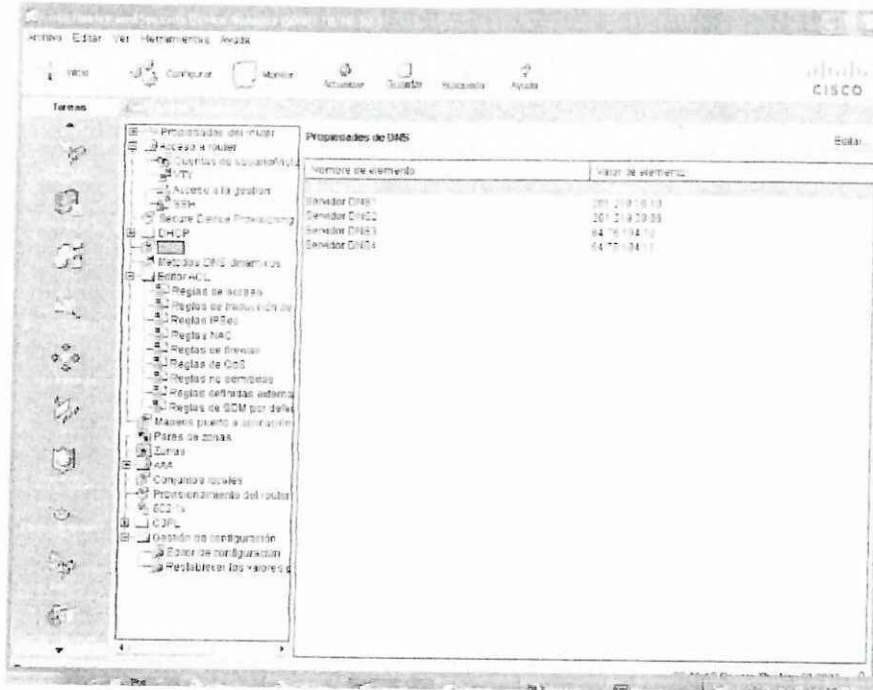
- La interfaz que será traducida es la FastEthernet0/0, que contiene la dirección IP 192.168.1.2
- Toda la red interna se traduce para el tráfico a la dirección IP 201.219.38.67
- Todos los pedidos realizados desde el exterior se traduce a la dirección física 201.219.38.66 a través de los puertos 25 y 80.

## TAREAS ADICIONALES

Toda la configuración realizadas en las diferentes opciones anteriormente indicadas se resumen en esta opción y da la posibilidad de realizar varios cambios adicionales. Las opciones se presenta en un menú desplegable y al lado izquierdo se visualiza la información de la opción seleccionada.

A continuación se presentan varias pantallas referentes a esta opción:







## CAPITULO II

### CONFIGURACIONES DEL ROUTER CISCO 2811 DEL CENTRO DE EXPERIMENTACION Y PRODUCCION SALACHE

#### INTRODUCCIÓN

Al finalizar esta unidad el Usuario del Router CISCO 2811 del CEYPSA estará en capacidad de:

- Identificar los trabajos de responsabilidad de un Router CISCO.
- Permitir el empleo y la maniobra operativa de las Router CISCO Serie 2811 en la Red de Datos del CEYPSA.
- Guiar a los usuarios técnicos en todas sus áreas.
- Comunicar los datos puntuales concernientes a la seguridad, fallas o puntos débiles y modificaciones.
- Formar y renovar conocimientos de técnicas de mantenimiento.

#### DE LA RED DE DATOS Y LABORATORIOS INFORMÁTICOS DEL CEYPSA

Son objetivos del Laboratorio de Informática del CEYPSA los siguientes:

- Brindar soporte técnico-Informático a la Administración de la Red de Datos y Laboratorios Informáticos del CEYPSA.
- Crear las condiciones necesarias para el óptimo uso de la Red de Datos y Laboratorios Informáticos del CEYPSA.
- Ofrecer apoyo para el desarrollo de los cursos, seminarios, programas y otras actividades de capacitación extracurricular conducidas por las diferentes dependencias facultativas del CEYPSA.

#### FUNCIONES DEL ENCARGADO DE RED DE DATOS Y LABORATORIOS INFORMÁTICOS DEL CEYPSA

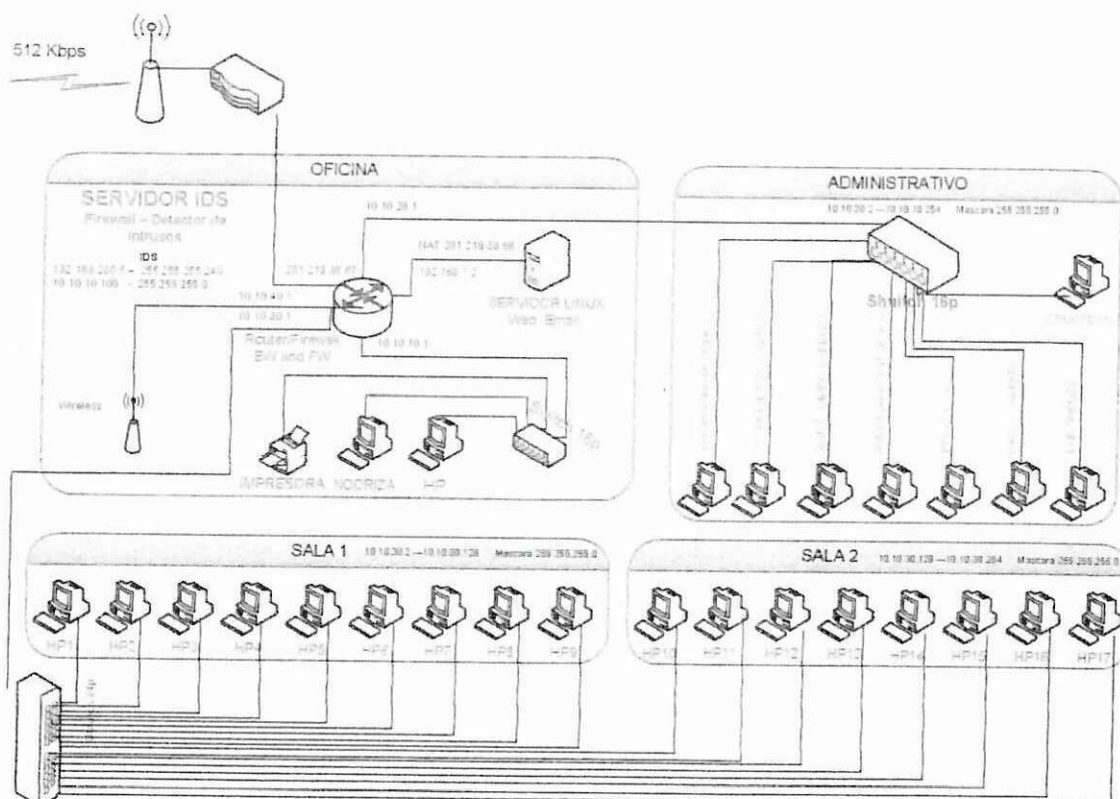
Son funciones del encargado del los Laboratorios Informáticos CEYPSA:

- Dirigir y Supervisar la Red de Datos y Laboratorios Informáticos, velando por el correcto y racional uso del los recursos, estableciendo coordinación permanente los usuarios de la Red de Datos a fin de asegurar el adecuado mantenimiento, estado de conservación y desarrollo de los mismos, velando por el buen estado y funcionamiento de los equipos e instalaciones disponibles.
- Aportar con ideas de juicio que sean necesarias para mantener e incrementar la operatividad y actualización de software existente.
- Prestar apoyo a los miembros de Universidad Técnica de Cotopaxi en los Servicios Informáticos requeridos y autorizados.



- Realizar tareas de mantenimiento preventivo de los Equipos en coordinación con los usuarios de la Red de Datos y el Director de Servicios Informáticos.

## DISEÑO DE LA RED DEL CEYPSA



Un vez configurado e instalado el Router Cisco 2811 en el Ceypsa la configuración queda establecida de la siguiente manera:

1. Considerando que el Router tiene 4 interfaces se han asignado de la siguiente manera:
  - **FastEthernet0/0.-** Tiene la IP 192.168.1.1 para conectarle al servidor Linux que tiene la IP 192.168.1.2
  - **FastEthernet0/1.-** Tiene la IP 201.219.38.67 para conectar al equipo del proveedor (antena)
  - **FastEthernet0/0/0.-** Tiene la IP 10.10.10.1 asignado para la VLAN de la oficina del Administrador de la Red
  - **FastEthernet0/0/1.-** Tiene la IP 10.10.20.1 asignado para la VLAN de las oficinas administrativas
  - **FastEthernet0/0/2.-** Tiene la IP 10.10.30.1 asignado para la VLAN de los laboratorios
  - **FastEthernet0/0/3.-** Tiene la IP 10.10.40.1 asignado para la VLAN de la red inalámbrica e edificio nuevo.



2. El diseño de la red que establecida de la siguiente manera:
- Conexión entre el servidor Linux con la interfaz 0/0 del Router, quedando asignado las direcciones IP de la siguiente manera:  
Interfaz del Router: 192.168.1.1 Máscara: 255.255.255.0  
Servidor Linux: 192.168.1.2 Máscara: 255.255.255.0
  - Conexión con el equipo del proveedor que permite el enlace a Internet se realiza en la interfaz 0/1 del Router quedando asignado las direcciones IP de la siguiente manera:  
Interfaz del Router: 201.219.35.67 Máscara: 255.255.255.248  
Equipo del proveedor: 201.219.35.65 Máscara: 255.255.255.248
  - VLAN de las oficinas del administrador de la red, quedando asignado las direcciones IP de la siguiente manera:  
Interfaz 0/0/0 del Router: 10.10.10.1 Máscara: 255.255.255.0  
IP de las estaciones: Desde la 10.10.10.2
  - VLAN de las oficinas administrativas, quedando asignado las direcciones IP de la siguiente manera:  
Interfaz 0/0/1 del Router: 10.10.20.1 Máscara: 255.255.255.0  
IP de las estaciones: Desde la 10.10.20.2
  - VLAN de los laboratorios, quedando asignado las direcciones IP de la siguiente manera:  
Interfaz 0/0/2 del Router: 10.10.30.1 Máscara: 255.255.255.0  
IP de las estaciones: Desde la 10.10.30.2
  - VLAN del wirelles y edificio adjunto, quedando asignado las direcciones IP de la siguiente manera:  
Interfaz 0/0/3 del Router: 10.10.40.1 Máscara: 255.255.255.0  
IP de las estaciones: Desde la 10.10.40.2
3. La configuración de los equipos en su interfaz de red queda establecida de la siguiente manera:
- VLAN 10.10.10.X
- Puerta de enlace: 10.10.10.1
  - DNS Preferido: 192.168.1.2
  - DNS Alternativo: 201.219.16.10
- VLAN 10.10.20.X
- Puerta de enlace: 10.10.20.1
  - DNS Preferido: 192.168.1.2
  - DNS Alternativo: 201.219.16.10
- VLAN 10.10.30.X
- Puerta de enlace: 10.10.30.1
  - DNS Preferido: 192.168.1.2
  - DNS Alternativo: 201.219.16.10
- VLAN 10.10.40.X



- Puerta de enlace: 10.10.40.1
- DNS Preferido: 192.168.1.2
- DNS Alternativo: 201.219.16.10

#### 4. Configuración del ancho de banda para las diferentes VLAN

VLAN 10

```
rate-limit output 128000 64000 92000 conform-action transmit exceed-action drop
```

VLAN 20

```
rate-limit output 64000 64000 64000 conform-action transmit exceed-action drop
```

VLAN 30

```
rate-limit output 256000 64000 128000 conform-action transmit exceed-action drop
```

VLAN 40

```
rate-limit output 64000 32000 64000 conform-action transmit exceed-action drop
```

### CONFIGURACIÓN DEL ROUTER 2811 DEL CEYPSA

Current configuration : 14726 bytes

!

#### \*\*\* Parámetros iniciales

version 12.4

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

#### \*\*\* definición del nombre del host

hostname CEYPSA

!

#### \*\*\* parámetros de arranque el Router , de donde toma la configuración de arranque

boot-start-marker

boot system flash c2800nm-advsecurityk9-mz.124-11.T.bin

boot-end-marker

!

#### \*\*\* establecimiento de la clave de ingreso

logging buffered 52000



```
enable password *****
```

```
!  
no aaa new-model  
clock timezone Bogota -5  
no ip source-route  
ip tcp synwait-time 10
```

```
!  
!  
ip cef  
!  
!
```

**\*\*\*\* se establece las direcciones IP de los DNS**

```
no ip bootp server  
ip domain name CEYPSA.utc.edu.ec  
ip name-server 201.219.16.10  
ip name-server 201.219.38.66  
ip name-server 64.76.194.10  
ip name-server 64.76.194.11
```

```
!  
multilink bundle-name authenticated  
!
```

```
!  
crypto pki trustpoint TP-self-signed-3911914078  
enrollment selfsigned  
subject-name cn=IOS-Self-Signed-Certificate-3911914078  
revocation-check none  
rsa-keypair TP-self-signed-3911914078
```

```
!  
crypto pki certificate chain TP-self-signed-3911914078  
certificate self-signed 01  
30820250 308201B9 A0030201 02020101 300D0609 2A864886 F70D0101 04050030  
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274  
69666963 6174652D 33393131 39313430 3738301E 170D3037 30393239 31363330  
34355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649  
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 39313139  
31343037 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281  
8100C63C 4062B775 BC85E840 7A3220BF 78FE8C29 25012113 563A808F  
37F387BF  
CE7D58E6 A5CCAACC 25B7DC8D 956D7A2D F31BEB36 7406C5FB 3AE82042  
10CF68BE  
C5C710EF 1DDC5D75 F58E8CEE 2F695BBE 85AC5F88 42020E24 A7132599  
BC974991  
A5ADDBDA D36B5B2C 5D0EDB18 04B27BE5 1E8B107B E70670D5 21FCA6A7  
8926D3B9
```



```
9E790203 010001A3 78307630 0F060355 1D130101 FF040530 030101FF 30230603
551D1104 1C301A82 18434559 5053412E 63657970 73612E75 74632E65 64752E65
63301F06 03551D23 04183016 8014077C A50DD6D8 04434CE9 67BEA0E5
11DD8FC9
6B0E301D 0603551D 0E041604 14077CA5 0DD6D804 434CE967 BEA0E511
DD8FC96B
0E300D06 092A8648 86F70D01 01040500 03818100 32B0FD3F 8B63C974
74EECD53
9622DE58 622B62FA 3C0ABA28 4850B916 ED398B4B 79222E24 1FB5BD7E
0C1C78B2
CF8DEB22 813844DD F141C4CD 32B6BC2E 3FA73693 E8A2FC40 171CEF1C
187557D5
AD81255E D8385B77 4770DD94 E28B1440 39467F05 3D6E3425 72B36877
51810A13
2574A1D7 8BFEED08 FA796684 1DA4A241 AB83F3B9
quit
!
!
```

\*\*\* Nombre de usuario con privilegios de administración  
username CEYPSA privilege 15 view root password 0 \*\*\*\*\*

```
!
!
```

\*\*\*\* definición de los puertos a verificar según los protocolos

```
class-map type inspect match-all sdm-nat-http-1
match access-group 103
match protocol http
class-map type inspect match-all sdm-nat-smtp-1
match access-group 102
match protocol smtp
class-map type inspect match-any SDM_TELNET
match access-group name SDM_TELNET
class-map type inspect match-any SDM_HTTP
match access-group name SDM_HTTP
class-map type inspect match-any SDM_SHELL
match access-group name SDM_SHELL
class-map type inspect match-any SDM_SSH
match access-group name SDM_SSH
class-map type inspect match-any SDM_HTTPS
match access-group name SDM_HTTPS
class-map type inspect match-any sdm-mgmt-cls-0
match class-map SDM_TELNET
match class-map SDM_HTTP
match class-map SDM_SHELL
```



```
match class-map SDM_SSH
match class-map SDM_HTTPS
class-map type inspect match-any sdm-cls-insp-traffic
match protocol cuseeme
match protocol dns
match protocol ftp
match protocol h323
match protocol https
match protocol icmp
match protocol imap
match protocol pop3
match protocol netshow
match protocol shell
match protocol realmedia
match protocol rtsp
match protocol smtp extended
match protocol sql-net
match protocol streamworks
match protocol tftp
match protocol vdolive
match protocol tcp
match protocol udp
class-map type inspect match-all sdm-insp-traffic
match class-map sdm-cls-insp-traffic
class-map type inspect match-any remote-access
match protocol tcp
match protocol udp
match protocol icmp
class-map type inspect match-any sdm-cls-icmp-access
match protocol icmp
match protocol tcp
match protocol udp
class-map type inspect match-any sdm-service-sdm-inspect-1
match protocol https
match protocol http
match protocol msnmsgr
match protocol aol
match protocol ymsgr
class-map type inspect match-all sdm-cls-sdm-permit-1
match class-map remote-access
match access-group name access
class-map type inspect match-any sdm-dmz-protocols
match protocol http
match protocol pop3s
match protocol ftp
match protocol smtp
```



```
match protocol https
match protocol imaps
class-map type inspect match-all sdm-dmz-traffic
match access-group name dmz-traffic
match class-map sdm-dmz-protocols
class-map type inspect match-all sdm-mgmt-cls-sdm-permit-0
match class-map sdm-mgmt-cls-0
match access-group 106
class-map type inspect match-all sdm-icmp-access
match class-map sdm-cls-icmp-access
class-map type inspect match-any web
match protocol http
match protocol https
match protocol smtp
match protocol imap
match protocol imaps
match protocol imap3
match protocol pop3
match protocol pop3s
match protocol msnmsgr
class-map type inspect match-all sdm-invalid-src
match access-group 101
match class-map web
class-map type inspect match-all sdm-protocol-http
match class-map sdm-service-sdm-inspect-1
!
```

**\*\*\* Establecimiento de políticas par a las diferentes zonas**

```
policy-map type inspect sdm-permit-icmpreply
class type inspect sdm-icmp-access
inspect
class class-default
pass
policy-map type inspect sdm-pol-NATOutsideToInside-1
class type inspect sdm-nat-smtp-1
inspect
class type inspect sdm-nat-http-1
inspect
class class-default
policy-map type inspect sdm-inspect
class type inspect sdm-invalid-src
inspect
class type inspect sdm-insp-traffic
inspect
class type inspect sdm-protocol-http
```



```
inspect
class class-default
policy-map type inspect sdm-permit
class type inspect sdm-cls-sdm-permit-1
inspect
class type inspect sdm-mgmt-cls-sdm-permit-0
inspect
class class-default
policy-map type inspect sdm-permit-dmzservice
class type inspect sdm-dmz-traffic
inspect
class type inspect sdm-nat-smtp-1
inspect
class type inspect sdm-nat-http-1
inspect
class class-default
!
```

### \*\*\* Definición de las zonas de seguridad

```
zone security dmz-zone
zone security out-zone
zone security in-zone
zone-pair security sdm-zp-self-out source self destination out-zone
service-policy type inspect sdm-permit-icmpreply
zone-pair security sdm-zp-NATOutsideToInside-1 source out-zone destination in-zone
service-policy type inspect sdm-pol-NATOutsideToInside-1
zone-pair security sdm-zp-out-dmz source out-zone destination dmz-zone
service-policy type inspect sdm-permit-dmzservice
zone-pair security sdm-zp-out-self source out-zone destination self
service-policy type inspect sdm-permit
zone-pair security sdm-zp-in-dmz source in-zone destination dmz-zone
service-policy type inspect sdm-permit-dmzservice
zone-pair security sdm-zp-in-out source in-zone destination out-zone
service-policy type inspect sdm-inspect
!
!
!
!
!
```

### \*\*\* Configuración de cada de una de las interfaces del Router, configuración de las Vlan

```
interface Null0
no ip unreachable
!
```



```
interface FastEthernet0/0
description DMZ$FW_DMZ$$ETH-LAN$
ip address 192.168.1.1 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp
ip nat inside
no ip virtual-reassembly
zone-member security dmz-zone
ip route-cache flow
duplex auto
speed auto
!
interface FastEthernet0/1
description WAN$FW_OUTSIDE$$ETH-LAN$
ip address 201.219.38.67 255.255.255.248
ip verify unicast reverse-path
no ip redirects
no ip unreachable
no ip proxy-arp
ip nat outside
no ip virtual-reassembly
zone-member security out-zone
ip route-cache flow
duplex half
speed 10
!
interface FastEthernet0/0/0
description Oficina
switchport access vlan 10
!
interface FastEthernet0/0/1
description Administracion
switchport access vlan 20
!
interface FastEthernet0/0/2
description Salas
switchport access vlan 30
!
interface FastEthernet0/0/3
description Wireless
switchport access vlan 40
!
interface Vlan1
ip address 10.100.100.1 255.255.255.252
no ip redirects
```



```
no ip unreachable
no ip proxy-arp
ip route-cache flow
!
interface Vlan10
description Oficina$FW_INSIDES
ip address 10.10.10.1 255.255.255.0
ip access-group 107 in
no ip redirects
no ip unreachable
no ip proxy-arp
ip nat inside
ip virtual-reassembly
rate-limit output 128000 64000 92000 conform-action transmit exceed-action drop
zone-member security in-zone
ip route-cache flow
!
interface Vlan20
description Administracion$FW_INSIDES
ip address 10.10.20.1 255.255.255.0
ip access-group 108 in
no ip redirects
no ip unreachable
no ip proxy-arp
ip nat inside
ip virtual-reassembly
rate-limit output 64000 64000 64000 conform-action transmit exceed-action drop
zone-member security in-zone
ip route-cache flow
!
interface Vlan30
description Salas$FW_INSIDES
ip address 10.10.30.1 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp
ip nat inside
ip virtual-reassembly
rate-limit output 256000 64000 128000 conform-action transmit exceed-action dro
p
zone-member security in-zone
ip route-cache flow
!
interface Vlan40
description Wireless$FW_INSIDES
ip address 10.10.40.1 255.255.255.0
```



```
no ip redirects
no ip unreachable
no ip proxy-arp
ip nat inside
ip virtual-reassembly
rate-limit output 64000 32000 64000 conform-action transmit exceed-action drop
zone-member security in-zone
ip route-cache flor
!
```

**\*\*\* Parámetros para el ruteo**

```
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1
ip route 0.0.0.0 0.0.0.0 201.219.38.65
!
```

**\*\*\* Parámetros de la configuración del NAT**

```
ip http server
ip http access-class 1
ip http secure-server
ip nat inside source list 100 interface FastEthernet0/1 overload
ip nat inside source static tcp 192.168.1.2 25 201.219.38.66 25 extendable
ip nat inside source static tcp 192.168.1.2 80 201.219.38.66 80 extendable
!
```

**\*\*\*\* Configuración de las políticas del NAT**

```
ip access-list extended SDM_HTTP
remark SDM_ACL Category=0
permit tcp any any eq www
ip access-list extended SDM_HTTPS
remark SDM_ACL Category=0
permit tcp any any eq 443
ip access-list extended SDM_SHELL
remark SDM_ACL Category=0
permit tcp any any eq cmd
ip access-list extended SDM_SSH
remark SDM_ACL Category=0
permit tcp any any eq 22
ip access-list extended SDM_TELNET
remark SDM_ACL Category=0
permit tcp any any eq telnet
ip access-list extended access
remark SDM_ACL Category=128
permit ip any host 10.254.0.248
ip access-list extended dmz-traffic
remark SDM_ACL Category=1
```



```
permit ip any host 192.168.1.1  
permit ip any host 192.168.1.2
```

\*\*\* **Definición de las lista de control de acceso**

```
access-list 1 remark Auto generated by SDM Management Access featurre  
access-list 1 remark SDM_ACL Category=1  
access-list 1 permit 10.10.20.0 0.0.0.255  
access-list 1 permit 10.10.10.0 0.0.0.255  
access-list 1 permit 201.219.38.0 0.0.0.255  
access-list 100 remark SDM_ACL Category=128  
access-list 100 permit ip host 255.255.255.255 any  
access-list 100 permit ip 127.0.0.0 0.255.255.255 any  
access-list 100 permit ip 10.10.50.0 0.0.0.255 any  
access-list 100 permit ip 10.10.40.0 0.0.0.255 any  
access-list 100 permit ip 10.10.30.0 0.0.0.255 any  
access-list 100 permit ip 10.10.20.0 0.0.0.255 any  
access-list 100 permit ip 10.10.10.0 0.0.0.255 any  
access-list 100 permit ip 201.219.38.64 0.0.0.7 any  
access-list 100 permit ip 192.168.1.0 0.0.0.255 any  
access-list 101 remark SDM_ACL Category=128  
access-list 101 permit ip host 255.255.255.255 any  
access-list 101 permit ip 127.0.0.0 0.255.255.255 any  
access-list 101 permit ip 10.10.20.0 0.0.0.255 any  
access-list 101 permit ip 10.10.30.0 0.0.0.255 any  
access-list 101 permit ip 10.254.0.0 0.0.0.255 any  
access-list 101 permit ip 10.10.40.0 0.0.0.255 any  
access-list 101 permit ip 192.168.1.0 0.0.0.255 any  
access-list 101 permit ip 10.10.10.0 0.0.0.255 any  
access-list 102 remark SDM_ACL Category=0  
access-list 102 permit ip any host 192.168.1.2  
access-list 103 remark SDM_ACL Category=0  
access-list 103 permit ip any host 192.168.1.2  
access-list 104 remark Auto generated by SDM Management Access feature  
access-list 104 remark SDM_ACL Category=1  
access-list 104 permit tcp 201.219.38.0 0.0.0.255 host 201.219.38.67 eq telnet  
access-list 104 permit tcp 201.219.38.0 0.0.0.255 host 201.219.38.67 eq 22  
access-list 104 permit tcp 201.219.38.0 0.0.0.255 host 201.219.38.67 eq www  
access-list 104 permit tcp 201.219.38.0 0.0.0.255 host 201.219.38.67 eq 443  
access-list 104 permit tcp 201.219.38.0 0.0.0.255 host 201.219.38.67 eq cmd  
access-list 104 deny tcp any host 201.219.38.67 eq telnet  
access-list 104 deny tcp any host 201.219.38.67 eq 22  
access-list 104 deny tcp any host 201.219.38.67 eq www  
access-list 104 deny tcp any host 201.219.38.67 eq 443  
access-list 104 deny tcp any host 201.219.38.67 eq cmd  
access-list 104 deny udp any host 201.219.38.67 eq snmp
```



```
access-list 104 permit ip any any
access-list 105 remark Auto generated by SDM Management Access feature
access-list 105 remark SDM_ACL Category=1
access-list 105 permit ip 10.10.20.0 0.0.0.255 any
access-list 105 permit ip 10.10.10.0 0.0.0.255 any
access-list 105 permit ip 201.219.38.0 0.0.0.255 any
access-list 106 remark Auto generated by SDM Management Access feature
access-list 106 remark SDM_ACL Category=1
access-list 106 permit ip 201.219.38.0 0.0.0.255 host 10.254.0.248
access-list 107 remark Auto generated by SDM Management Access feature
access-list 107 remark SDM_ACL Category=1
access-list 107 permit tcp 10.10.10.0 0.0.0.255 host 10.10.10.1 eq telnet
access-list 107 permit tcp 10.10.10.0 0.0.0.255 host 10.10.10.1 eq 22
access-list 107 permit tcp 10.10.10.0 0.0.0.255 host 10.10.10.1 eq www
access-list 107 permit tcp 10.10.10.0 0.0.0.255 host 10.10.10.1 eq 443
access-list 107 permit tcp 10.10.10.0 0.0.0.255 host 10.10.10.1 eq cmd
access-list 107 deny tcp any host 10.10.10.1 eq telnet
access-list 107 deny tcp any host 10.10.10.1 eq 22
access-list 107 deny tcp any host 10.10.10.1 eq www
access-list 107 deny tcp any host 10.10.10.1 eq 443
access-list 107 deny tcp any host 10.10.10.1 eq cmd
access-list 107 deny udp any host 10.10.10.1 eq snmp
access-list 107 permit ip any any
access-list 108 remark Auto generated by SDM Management Access feature
access-list 108 remark SDM_ACL Category=1
access-list 108 permit tcp 10.10.20.0 0.0.0.255 host 10.10.20.1 eq telnet
access-list 108 permit tcp 10.10.20.0 0.0.0.255 host 10.10.20.1 eq 22
access-list 108 permit tcp 10.10.20.0 0.0.0.255 host 10.10.20.1 eq www
access-list 108 permit tcp 10.10.20.0 0.0.0.255 host 10.10.20.1 eq 443
access-list 108 permit tcp 10.10.20.0 0.0.0.255 host 10.10.20.1 eq cmd
access-list 108 deny tcp any host 10.10.20.1 eq telnet
access-list 108 deny tcp any host 10.10.20.1 eq 22
access-list 108 deny tcp any host 10.10.20.1 eq www
access-list 108 deny tcp any host 10.10.20.1 eq 443
access-list 108 deny tcp any host 10.10.20.1 eq cmd
access-list 108 deny udp any host 10.10.20.1 eq snmp
access-list 108 permit ip any any
no cdp run
!
access-list 108 permit ip any any
no cdp run
!
!
!
control-plane
```



```
!  
!  
  
*** Parámetros de seguridad para el acceso del Router  
line con 0  
line aux 0  
line vty 0 4  
access-class 105 in  
exec-timeout 60 0  
password *****  
login  
transport input telnet ssh  
transport output telnet ssh  
!  
scheduler allocate 20000 1000  
!  
end
```

#### LICENCIA

COPYRIGHT (C) 2008 Vaca A. José, Castellano M. Paúl.  
UNIVERSIDAD TECNICA DE COTOPAXI  
CARRERA DE CIENCIAS DE LA INGENIERIA Y APLICADAS  
PROYECTO DE CONFIGURACION DE UN ROUTER PARA OPTIMIZAR LA  
ADMINISTRACION DE LA RED DE DATOS DEL CEYPSA

Se otorga permiso para reproducir total o parcialmente este documento, siempre y cuando se cite la fuente. Cualquier modificación de este documento deberá ser aprobada por los autores.