



DESARROLLO DEL PROTOTIPO DE UN SISTEMA PARA EL MANEJO DE EQUIPOS DE LA RED CENTROSUR IP/MPLS

INDICE

CAPÍTULO 1, INTRODUCCION	- 7 -
1.1. Antecedentes	- 8 -
1.2. Justificación	- 9 -
1.3. Objetivos	- 11 -
1.4. Problemas Resueltos	- 12 -
CAPÍTULO 2, MARCO TEORICO	- 15 -
2.1. Gestión de Redes de Comunicación	- 15 -
2.2. Tecnologías de comunicación	- 23 -
2.4. Protocolos de Administración	- 35 -
CAPÍTULO 3, DISEÑO E IMPLEMENTACIÓN	- 53 -
3.1. Análisis	- 53 -
3.2. Diseño	- 94 -
3.3. Implementación	- 147 -
3.3. Pruebas	- 178 -
CAPÍTULO 4, CONCLUSIONES	- 183 -
4.1. Conclusiones	- 183 -
4.2. Recomendaciones	- 185 -

RESUMEN

El sistema prototipo desarrollado para la Empresa Eléctrica Regional Centrosur tiene como principal objetivo la integración de las herramientas que permitan el desarrollo de un sistema para el **monitoreo** a través del uso del protocolo *Simple Network Management Protocol* y **manejo** mediante el uso de software de automatización, de los equipos de la red *Multiprotocol Label Switching* implementada en la ciudad de Cuenca, que actualmente brinda servicios de internet y datos a sus clientes. Los módulos de gestión de la configuración y monitoreo que posee el sistema automatizan las tareas que se realizaban de manera manual, integrando la información de; clientes, usuarios e información administrativa de la red de datos, facilitando la ejecución de los procesos de configuración y registrando las tareas que se llevan a cabo en la administración de la Red.

PALABRAS CLAVE:

Red, Telecomunicaciones, SNMP, MPLS, Automatización, ExpectJ, NMS



Universidad de Cuenca

UNIVERSIDAD DE CUENCA
FACULTAD DE INGENIERÍA
ESCUELA DE INFORMÁTICA

**DESARROLLO DEL PROTOTIPO DE UN SISTEMA PARA EL MANEJO DE
EQUIPOS DE LA RED CENTROSUR IP/MPLS**



Tesis previa a la obtención
del título de Ingeniero de Sistemas

AUTOR:

LUIS PAUL GARCIA ANGUISACA

DIRECTORA:

ING. PRISCILA CEDILLO

ASESOR:

ING. DIEGO UNKUCH

Cuenca - Ecuador

Junio 2011



**“LAS OBRAS DE CONOCIMIENTO DEBEN SER LIBRES, NO HAY
EXCUSAS PARA QUE NO SEA ASI”**

RICHARD STALLMAN



AGRADECIMIENTO

Para mi Familia, mi Padre Luis, mis hermanas Mercy, Jessica y Pamela y especialmente a mi Madre Ligia, ya que gracias a su apoyo y dedicación he alcanzado las metas que he planteado en la vida. Siempre han sabido guiarme con su ejemplo de esfuerzo y trabajo.

DEDICATORIA

Este trabajo de grado va dedicado a la Facultad de Ingeniería especialmente a mi Profesora la Ingeniera Priscila Cedillo mi directora de tesis que junto con mi asesor el Ing Diego Unkuch de la Empresa Eléctrica Regional Centrosur han sabido brindarme los conocimientos necesarios y guiarme en el desarrollo del presente trabajo.



CONTENIDO

1	CAPITULO I – INTRODUCCIÓN	7
1.1	ANTECEDENTES	8
1.2	JUSTIFICACIÓN	9
1.3	OBJETIVOS	11
1.4	PROBLEMAS RESUELTOS	12
2	CAPÍTULO II: MARCO TEÓRICO	16
2.1	GESTIÓN DE REDES DE COMUNICACIÓN	16
2.1.1	<i>Modelo de Gestión FCAPS</i>	16
2.1.2	<i>NMS disponibles en el mercado</i>	19
2.2	TECNOLOGÍAS DE COMUNICACIÓN	22
2.2.1	<i>Redes multi-servicios</i>	22
2.2.2	<i>Modelo Jerárquico de Redes Cisco</i>	24
2.2.3	<i>MPLS Multi Protocol Label Switching</i>	27
2.3	PROTOCOLOS DE ADMINISTRACIÓN	35
2.3.1	<i>SNMP Simple Network Management Protocol</i>	35
3	CAPITULO III: DISEÑO E IMPLEMENTACION DEL PROTOTIPO	53
3.1	ANÁLISIS	53
3.1.1	<i>Requerimientos</i>	53
3.1.2	<i>Análisis y estudio de la Red Centrosur IP/MPLS</i>	59
3.1.3	<i>Breve descripción de los equipos de la Red MPLS</i>	69
3.1.4	<i>Selección de Herramientas de Software Libre</i>	74
3.2	DISEÑO	93
3.2.1	<i>Arquitectura del sistema</i>	93
3.2.2	<i>Actores</i>	98
3.2.3	<i>Casos de Uso</i>	99
3.2.4	<i>Diagramas de secuencia</i>	117
3.3	IMPLEMENTACIÓN	141
3.3.1	<i>Modelo de Red IP/MPLS Virtual</i>	141
3.3.2	<i>Capa de Datos</i>	143
3.3.3	<i>Procesos de Configuración de Equipos</i>	152
3.3.4	<i>Procesos de Monitoreo de Equipos</i>	163
3.3.5	<i>Interfaz</i>	165
3.3.6	<i>Ambiente de Producción</i>	167
3.3.7	<i>Entorno Virtual</i>	167
3.4	PRUEBAS	171
3.4.1	<i>Pruebas</i>	171
4	CAPITULO IV: CONCLUSIONES Y RECOMENDACIONES	179
4.1	CONCLUSIONES	179
4.2	RECOMENDACIONES	181
4.3	TRABAJOS FUTUROS	182
4.4	GLOSARIO	183
4.5	ANEXOS	187
4.6	BIBLIOGRAFÍA	233



CAPITULO I

INTRODUCCIÓN



1 Capítulo I – Introducción

Las redes de telecomunicaciones actualmente permiten el acceso a diferentes servicios como datos, voz, video y demás, debido a esto se presenta la necesidad de contar de manera unificada con estas prestaciones, el rediseño de las aplicaciones de software existente para llevar a cabo esta tarea supondría un gasto tanto en tiempo como en dinero. Igualmente sucede con el hardware que está funcionando hoy en día, de ahí la necesidad de contar con protocolos a nivel de red que nos lleven a esta convergencia. Las redes multi-servicio tienen la capacidad de establecer contenidos y servicios personalizados, por lo que actualmente se han considerado tecnologías como *Multiprotocol Label Switching*, MPLS que permite a los operadores explotar estas redes para ofrecer niveles previsibles de QoS, latencia y fiabilidad para todo tipo de aplicaciones multimedia. IP/MPLS es un mecanismo de transporte de datos para redes multi-servicios desarrollado por la *Internet Engineering Task Force (IETF)*, diseñado con el propósito de unificar el servicio de transporte de datos para las redes basadas en circuitos y las redes basadas en paquetes mediante el uso de etiquetas. Siendo su utilidad fundamental converger el transporte de diferentes tipos de tráfico. MPLS realiza estas funcionalidades mediante la interacción de varios elementos físicos entre los cuales están puntos de entrada y conmutadores que conforman un core central en el cual el enrutamiento está basado en etiquetas. Protocolos adaptados y especializados para este modo de trabajo junto con la correcta configuración de los equipos establecen un entorno idóneo para unificar el servicio de transporte de diferentes tipos de tráfico.



1.1 Antecedentes

La Empresa Eléctrica Regional Centrosur (EERCS) que actualmente está incursionando en la provisión de servicios de telecomunicaciones, con el afán de convertirse en el proveedor líder de servicios de internet, ha implementado la tecnología IP-MPLS, que le permite brindar servicios convergentes a sus clientes. Para realizar estas prestaciones, es necesaria la configuración de los equipos involucrados en la red, que al presente los operadores de red lo llevan a cabo de forma manual accediendo directamente a través de terminales a los routers y switches que conforman el core IP/MPLS. No se cuenta con un control de permisos sobre las tareas que se realizan en los equipos y sus responsables. La información de direccionamiento IP se está manejando a través de archivos Excel que se almacena de manera distribuida, el cálculo de subredes se realiza de forma manual. Así como para la asignación de las subredes a las respectivas interfaces de los equipos se llevan únicamente registros en archivos Excel. Para establecer la relación de los enlaces y clientes a los que se les fueron asignados, se utilizan archivos de texto. Al contar con una red diseñada para grandes proporciones su administración conlleva mucha complejidad, dicha administración que se lleva a cabo utilizando scripts escritos en archivos de texto plano, que presentan varios inconvenientes al momento de habilitar las configuraciones deseadas por lo que en la mayoría de los casos se deben realizar de manera manual accediendo directamente a los equipos mediante sesiones telnet, lo que aumenta el tiempo de implementación y configuración, en tareas que son netamente repetitivas.



Actualmente en la dirección de telecomunicaciones se cuenta únicamente con el sistema SITEL orientado a la comercialización, y no existe un sistema de administración que cubra los requerimientos y falencias anteriormente expuestas en el área operativa de configuraciones de la red que es una de las principales áreas funcionales de gestión de una red heterogénea como la red Centrosur IP /MPLS.

1.2 Justificación

En base a lo citado anteriormente, es precisa la implementación de un sistema que ayude en la administración de la red Centrosur IP/MPLS de la Empresa Eléctrica Regional Centrosur.

Se requiere un sistema que realice los procesos de configuración de la red que tendrán que ser centralizado, pero a su vez permitir acceso remoto desde cualquier lugar dentro o fuera de las instalaciones de la Empresa, debido a los servicios de soporte y alta disponibilidad que brinda Centrosur.

Para realizar las tareas de configuración se debe tener un acceso total a los equipos con privilegios de administración completos, por tanto, el sistema automáticamente tendrá que acceder mediante una sesión de consola remota con todos los privilegios, esto a través del uso de la tecnología TCL scripting lenguaje y específicamente aprovechando las funcionalidades de la extensión Expect que permite trabajar con herramientas interactivas como telnet o ssh usando pseudo terminales

Se requiere un registro para la relación existente entre el cliente y el enlace configurado en la red física, así como la información correspondiente a la



infraestructura física, como equipos utilizados para dicho enlace, e información lógica de comandos de configuración utilizados en la creación del enlace. Ya que esta información resulta de suma utilidad en el área operativa para tareas de mantenimiento, y que actualmente se lleva solamente en archivos de texto elaborados manualmente sin ningún tipo de control.

Se requiere de un sistema que automatice las tareas de respaldo y de configuración de los equipos mediante scripts, esto conjuntamente con un historial de dichas tareas. Ya que es necesaria una herramienta de backups de las configuraciones realizadas en la red.

Dada la forma de trabajo en la que el sistema se desempeñará es necesario un entorno gráfico de calidad, donde se pueda visualizar la red Centrosur IP/MPLS. Esto, que al ser implementado con el modelo de programación MVC (Modelo Vista Controlado) combinado con un ambiente de desarrollo de aplicaciones web RIA (Rich Internet Application), brinda a los usuarios un manejo intuitivo, fácil y eficiente de la aplicación.

Se requiere de un sistema que administre la información de direccionamiento, calculo de subredes y registros de direcciones ip utilizadas y disponibles que se utilizan en las configuraciones de red.

Es necesario el monitoreo de los equipos para tener conocimiento de la disponibilidad de los mismos a fin de poder trabajar sobre ellos, y reportes de información para los usuarios del área de operaciones en caso de que exista un fallo. Esto es necesario realizarlo mediante la implementación de un cliente SNMP (Simple Network Management Protocol).



Se requiere un sistema en el cual los usuarios tengan acceso y se les permita la ejecución de tareas según el rol que les fuere establecido, lo que facilitará la asignación de tareas y responsables.

Actualmente debido al mandato 1014 emitido por el gobierno se requiere la utilización de software libre por lo que el sistema será desarrollado en base a esta política.

1.3 Objetivos

Objetivo General

Elaborar el prototipo de un sistema que integre las tecnologías que permitan la automatización de los procesos de configuración de los equipos que conforman una red IP/MPLS, con una adecuada gestión de la información.

Objetivos Específicos

- Aprender la gestión de networking que requiere el protocolo IP/MPLS aplicado en un proveedor de servicios de internet.
- Aprender e investigar las tecnologías que permitan la implementación de un sistema de gestión de configuraciones y monitoreo de red.
- Aprender e investigar sobre las herramientas de software y su integración, en software libre, que permitan la implementación del prototipo del sistema de tesis.
- Automatizar las tareas de configuración de los equipos que conforman la red IP/MPLS.
- Consolidar la información de configuración con la información administrativa de los Clientes de Centronet..



- Monitorear de los equipos de la red, basado en la implementación de SNMP.
- Gestionar la información que será de utilidad para usuarios del área de operaciones, que les permitirá dar soporte en los equipos.

1.4 Problemas Resueltos

El sistema esta en capacidad de realizar las siguientes tareas:

Módulo de Configuración

- Gestión de enlaces MPLS de capa tres mediante scripts. Se automatizara la configuración de las VRFs basadas en las características propias de cada enlace ya sean estos de internet corporativos, datos o internet residencial.
- Gestión de VLANs, mediante scripts se automatizara la configuración de vlans y filtrado de puertos de los equipos.

Modulo de Network Utilities

- Gestión de Network Utilities: automatización de los procesos de traceroute, ping, nslookup mediante scripts. Herramientas usadas en las tareas de configuración y soporte.

Modulo de RespalDOS

- Gestión de Backups, se automatizara con scripts los procesos de respaldo de las configuraciones que están corriendo en los equipos y serán almacenadas en un servidor centralizado.

Modulo de Equipos



- Gestión de Equipos: que permitirá contar con una base de información de los equipos que se encuentran activos y forman parte del core de la red Centrosur IP/MPLS.

Modulo de Monitoreo

- El sistema realizará un monitoreo para tener conocimiento de los eventos presentados en los equipos que conforman el Core de la red Centrosur IP/MPLS.

Módulo de Clientes

- Gestión de Clientes, se leerá información de la base de datos de clientes con los que se establecerá una relación entre el cliente y los enlaces configurados en los equipos para proveerle servicio a dicho cliente. Al tratarse de un sistema prototipo se trabajará con información simulada de la Base de Datos manejada por el sistema de telecomunicaciones SITEL, encargado de la comercialización.

Módulo de Direccionamiento.

- Gestión de la información de direccionamiento ip versión cuatro (ipv4). Se implementara una Calculadora IP, almacenamiento de la información de Subredes de los nodos principales del core IP/MPLS. Y un registro de la asignación de direcciones ip de las subredes a vrf y vlans de clientes e interfaces de equipos.

Módulo de Usuarios.



Universidad de Cuenca

- Gestión de usuarios, diseño del manejo mediante roles de usuarios con privilegios de acceso a los diferentes módulos.



CAPITULO II

MARCO TEORICO



2 CAPÍTULO II: MARCO TEÓRICO

2.1 GESTIÓN DE REDES DE COMUNICACIÓN

2.1.1 Modelo de Gestión FCAPS

En el año 1997 la ISO (International Organization for Standardization) aplica el modelo FCAPS M.3400 (sucesor del M.3010) a redes de datos basadas en el modelo OSI como la estructura de gestión de redes de telecomunicaciones. Estructura que se conserva hasta nuestros días.

Podemos definir entonces a FCAPS como el modelo y *framework* de red de gestión de telecomunicaciones de ISO para la gestión de redes. Donde las áreas clave de función para el manejo de una red son definidas por la ISO como las siguientes:

F	Fault Management
C	Configuration Management
A	Accounting Management
P	Performance Management
S	Security Management

Figura 2.1 FCAPS

A continuación se realiza una descripción de las áreas funcionales de gestión

Gestión de Fallas



Entiéndase como la facilidad para la detección, aislamiento y corrección de operaciones anormales en las redes de telecomunicaciones. Además se considera el uso de análisis de tendencias para predecir errores de tal manera que la red siempre está disponible.

Cuando ocurre una falla o un evento de error, el componente de la red que lo está sufriendo enviará una notificación al operador de la red utilizando un protocolo propietario o abierto como SNMP que se verá con más detalle más adelante.

Gestión de Configuración

Esta área funcional tiene que encargarse de obtener información de la red y usarla para hacer ajustes a la configuración de los dispositivos de la red para proporcionar simplicidad y agilidad en las operaciones de interconexión de servicios de red. Además de permitir llevar un seguimiento de los cambios que se realizan a la configuración. Según las redes incrementan su tamaño, una tarea importante es la configuración automatizada.

Gestión de Cuentas o Administración

La gestión de las cuentas o también conocida como la gestión de la tarificación tienen como objetivo reunir las estadísticas de los usuarios clientes de la red. RADIUS, TACACS y DIAMETER son ejemplos de protocolos comúnmente utilizados para gestión de cuentas o tarificación.



Para redes no tarifadas, "administración" reemplaza a "cuentas". Los objetivos de la administración son gestionar los usuarios de la red autorizados para administrar, estableciendo nombres de usuarios, contraseñas, roles y permisos para realizar operaciones permitidas en los equipos.

Gestión de Rendimiento

La gestión de rendimiento determina la eficiencia y rendimiento de la red; estos valores se miden de acuerdo a:

- Throughput.- se define como la capacidad de la red para transmitir información, concretamente se habla de un volumen de información que fluye en una red de datos en un lapso de tiempo determinado
- Porcentaje de utilización.- el ancho de banda que se esta utilizando de la red
- Las tasas de error.- el numero de perdidas de paquetes o conexión por periodo de tiempo que sufre la red
- Tiempos de respuesta.- Se define como el tiempo transcurrido entre el momento en que se envía un mensaje de comunicación de datos hasta el momento en que se recibe una respuesta de dicho mensaje.

Para cumplir con estas funciones se utilizan generalmente software para monitoreo como MRTG, CACTI y otros



Gestión de Seguridad

La gestión de Seguridad implica la aplicación de los aspectos de seguridad esenciales del modelo OSI para operar redes de datos de una manera correcta y segura con procesos que controlen el acceso a recursos en la red. La seguridad de datos puede ser conseguida principalmente con la autenticación, el cifrado y la autorización, es decir un modelo conocido como AAA.

2.1.2 NMS disponibles en el mercado

Cacti Network Graphing

Cacti es una solución grafica de redes para el monitoreo de equipos, utiliza la funcionalidad grafica de las RRDtool (Round RobinDatabasetool), desarrollada en PHP, contiene plantillas de gráficos para presentación de estadísticas y recolección de datos, la recopilación de datos esta basada en el protocolo SNMP, posee también módulos para el manejo de usuarios del sistema.

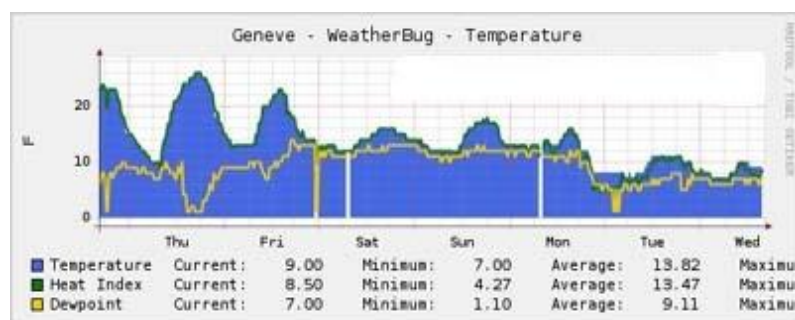


Figura 2.2: Cacti Network Graphing

Tiene una interfaz web que permite la gestión desde instalaciones del tamaño de una LAN hasta redes complejas con cientos de dispositivos.



Representar gráficamente los datos recolectados de monitoreo de equipos para características como: temperatura, throughput, voltaje entre otros.

La RRD tolos que están integradas al sistema se encargan del almacenamiento, procesamiento y grafico de datos recolectados vía SNMP. RRDtool usa sensores para medir los datos. Crea una base de datos, almacena los datos en ella, recupera estos datos y basándose en ellos, Cacti crea gráficos en formato PNG.

RRDtool es una herramienta que trabaja con una base de datos la cual la gestiona según el método Round-Robin que trata la base de datos como si fuese un círculo, sobrescribiendo los datos almacenados con anterioridad, siempre dependiendo de la cantidad de información que se quiera conservar como historial.

La Empresa Eléctrica actualmente tiene implementada la aplicación Cacti para el monitoreo de los equipos del core de la red Centrosur IP/MPLS donde se agregan manualmente los nodos o equipos a ser monitoreados.

Orión Network Performance Monitor

Orion Network Performance Monitor, monitorea y recoge datos de routers, switches, servidores, y cualquier otro dispositivo de red con capacidad SNMP. Monitorea la carga de CPU, utilización de memoria, y espacio en disco disponible entre otras características.



Orión permite ver gráficamente el estado de la red, permite la creación de informes periódicamente. Utiliza SNMP e ICMP y no requiere instalación de ningún hardware adicional o agentes de software en la red. Realiza la gestión de fallas con capacidad de alerta para saber exactamente cuando existan problemas de corte en la red o problema de rendimiento.

Dado que Orión esta basado en la web, cualquier personal ya sean estos ingenieros, directivos, personal administrativo o inclusive clientes pueden tener acceso inmediato a la situación actual de la red.

Una de las características importantes de Orión es la de ser escalable - lo que le permite supervisar unos cuantos dispositivos desde un único servidor hasta una topología de ISP.

Este es el par comercial de Cacti que incluye soporte y garantías, a mas de una serie de herramientas adicionales y procesos automáticos que en Cacti se realizan de manera manual, que justifica el valor del producto el cual depende del tipo de licencias que limitan las funcionalidades del sistema en el monitoreo de equipos.

Análisis

Existen varias soluciones tanto de software libre como openNMS y legacy como Orion, que en su mayoría se enfocan en el monitoreo dejando la gestión de configuración de lado.

Algo importante a tomar en consideración es el hecho de que la mayoría de este software está desarrollado en php que a pesar de ser un



lenguaje de código abierto limita la integración con sistemas que están desarrollados en otras plataformas como Java que es el caso de la Empresa Eléctrica Regional Centrosur ya que posee todos sus sistemas implementados en esta plataforma.

Ninguna de estas herramientas posee módulos de gestión de configuración que puedan ser adaptados fácilmente a las necesidades funcionales del personal operativo de la Empresa. Siendo esto aun mas difícil al tratarse de una tecnología para un core de equipos como el de la red Centrosur IP/MPLS.

2.2 TECNOLOGÍAS DE COMUNICACIÓN

2.2.1 Redes multi-servicios

En vista del crecimiento que ha tenido internet y los servicios que a través de este medio se proveen, los operadores han dirigido su inversión tanto en tecnología como en personal que les permita brindar estos servicios a sus clientes.

El modelo actual de redes basadas en IP trata a todos los paquetes por igual, ya que todos se trasladan con el principio del mejor esfuerzo, “El primero en llegar el primero en despacharse”, La trayectoria que tome un paquete depende de las tablas de enrutamiento que manejan los routers y tomando en cuenta también la carga general de la red.

La tarea principal de los protocolos de QoS es brindar diferentes prioridades a flujos de datos de manera que se garanticen una calidad



de servicio diferenciada en el transporte de los mismos. Actualmente hay 2 modelos que se utilizan para implementar QoS:

- Servicios integrados (IntServ)
- Servicios distinguidos (DiffServ)

Servicios Integrados

Los Servicios Integrados como su nombre lo indica realizan una transmisión de datos integrando los elementos de red para que trabajen de manera conjunta realizando reserva de recursos de la red como el ancho de banda por ejemplo para lograr que una conexión establecida por medio de este modelo obtenga la calidad de servicio requerida. Para trabajar con este modelo los routers involucrados deben almacenar información sobre los flujos, de tal manera que cuando un paquete es recibido se analiza para saber a que flujo corresponde y cual es el tratamiento que se le tiene que dar.

El protocolo RSVP esta basado en el modelo de IntServ. Este es un protocolo de reserva de recursos tales como el ancho de banda por ejemplo y demás recursos que influyen en la QoS, RSVP tiene una escalabilidad limitada, por lo que su implementación en el ambiente de Internet es compleja e inadecuada como una solución de QoS.

Servicios Distinguidos

Mientras que IntServ ofrece la capacidad de reservar de recursos conjuntamente con el establecimiento previo de la ruta, con eso define un modelo que trabaja bien en redes de menor tamaño; la arquitectura



distinguida de los servicios o DiffServ esta diseñada para redes grandes y de gran escalabilidad, y por supuesto para su uso en Internet.

Los Servicios diferenciados realizan un análisis de los flujos de datos, es decir en un flujo a cada paquete se lo marca y se lo clasifica para que reciba un tratamiento por salto que se denomina PHB o Per-Hop Behavior, Tal clasificación se lleva a cabo en los extremos de un dominio gestionado mediante Servicios Diferenciados. Cuando hablamos de un dominio DiffServ nos referimos a un grupo de routers que están interconectados y se define a dicho dominio por medio de los routers que se encuentran en el limite y quienes son los encargados de marcar los paquetes, mientras los routers que se encuentran en el interior realizan el reenvío basados en los valores de DiffServ que fueron establecidos en los paquetes al entrar en el dominio

Un entorno típico de DiffServ es el protocolo IP/MPLS en el cual se pueden identificar claramente los elementos involucrados en este modelo. Dicho protocolo se vera con detalle mas adelante.

2.2.2 Modelo Jerárquico de Redes Cisco.

El modelo Jerárquico en capas para el diseño de la red define funciones específicas dentro de cada capa, ya que las redes grandes pueden ser extremadamente complejas e incluir múltiples protocolos y tecnologías.

No necesariamente los routers en cada capa deben estar separados, un mismo equipo podría incluso realizar funciones de varias capas. Es asi



que el modelo Jerárquico de Cisco define tres capas principales que se describen a continuación.

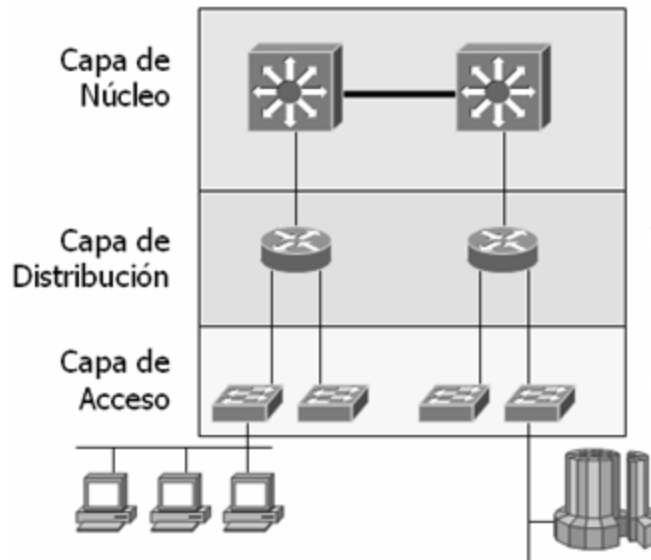


Figura 2.3 Modelo Jerárquico Cisco

Capa de Acceso

La capa de acceso se encarga de realizar la conmutación de paquetes, permite y controla directamente el acceso de los usuarios a los recursos de la red, también llamada capa de escritorio o de usuario. En esta capa se definen los dominios de colisión. Y se configura el ruteo de manera estática.

Capa de Distribución

La principal función de la capa de distribución es el enrutamiento o routing; esta capa también llamada *workgroup layer* proveer ruteo, acceso a la red WAN y determina que paquetes deben llegar al Core.



Los administradores de la red utilizan esta capa para configurar las políticas de red, en este sentido además del ruteo, también se implementan: access-list, filtrado de paquetes, cola de espera, etc. Aparte de las políticas mencionadas también se implementan las medidas de seguridad de red ya sean estos de tipo proxy o NAT y Firewalls que son muy importantes a la hora de evitar problemas de ataques informáticos.

Es muy común implementar funciones en esta capa que son exclusivas de otras capas y en este sentido se debe tener cuidado a la hora de realizar las configuraciones para tener un modelo Jerárquico correcto.

Capa de Core

El Núcleo de la red o core layer como también se la conoce, tiene la única función de conmutar grandes cantidades de tráfico a través de la red tan rápido como sea posible pero de manera segura, por lo que la latencia y la velocidad son factores importantes en esta capa. Entendiendo el concepto de latencia como la suma de retardos temporales dentro de la red y el tiempo que le toma a un paquete llegar desde un punto de la red a otro como la velocidad. Podemos entonces decir que es la parte más sensible de la red ya que si falla se afecta a todos los usuarios conectados a la red, por lo que la tolerancia a errores debe ser alta.



Para contar con un core eficiente es recomendable evitar aumentar el número de dispositivos en el *Core*. Y en el caso de que consideremos que la capacidad del Core es insuficiente, lo que se debe hacer es aumentar la plataforma de hardware de los equipos que trabajan en el núcleo.

2.2.3 MPLS Multi Protocol Label Switching

MPLS es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC3031¹. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Por tanto se utiliza para transportar diferentes tipos de tráfico como voz y paquetes IP.

(wikipedia, 2011)

Funcionamiento de MPLS

Un dominio MPLS lo podemos definir como grupo de routers denominados LSR (Label switched routers), este mecanismo de transporte se basa en el modelo DiffServ y por tanto esta tasado por los routers de borde, los cuales junto con los routers internos conmutan paquetes según sea la etiqueta que se haya asignado. Dicha etiqueta define un flujo de paquetes entre dos extremos del dominio MPLS y en el caso de la multidifusión entre un extremo fuente y varios destinos.

¹ RFC 3031 - Multiprotocol Label Switching Architecture, Definición de la IETF sobre la Arquitectura de MPLS



Cada flujo de datos presente en el dominio MPLS se denomina FEC (clase de equivalencia de reenvío - Forwarding equivalence class) que no es mas que un grupo de paquetes que siguen un mismo camino. De donde podemos decir que MPLS es orientada a la conexión. Es en la FEC que se definen los parámetros de QoS de ese flujo que especifican la cantidad de recursos asignados a los paquetes de ese flujo

La figura 2.4 describe el funcionamiento de MPLS:

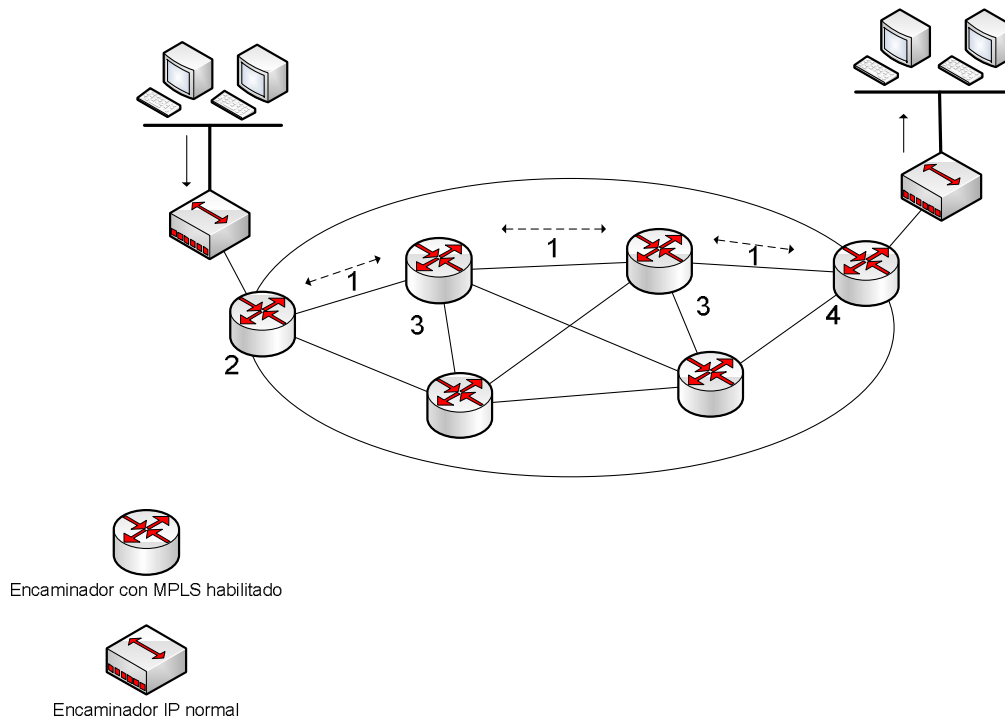


Figura 2.4 Funcionamiento MPLS

Descripción:

1. El paso inicial es definir una ruta en la red conocida como LSP (ruta conmutada de etiquetas – label switched path) y también



definir los parámetros QoS para la ruta. Los parámetros de QoS a definir son:

- a. Cuantos recursos asignar a dicha ruta.
- b. Que políticas de colas y descarte de paquetes establecer en cada LSR.

Para determinar esto se intercambia la siguiente información entre routers

- a. Se utiliza OSPF para intercambiar información de encaminamiento y alcance.
 - b. Se utiliza un protocolo de distribución de etiquetas como LDP o RSVP.
2. Cuando un paquete ingresa al dominio MPLS se procesa para determinar sus parámetros de QoS, el LSR coopera con los demás LSR para generar un LSP en particular para el paquete y por tanto a una FEC, asigna también la etiqueta adecuada al paquete y lo reenvía.
 3. Cada LSR que recibe un paquete retira la etiqueta entrante y le asocia la correspondiente etiqueta de salida y reenvía el paquete por la ruta LSP.
 4. El LSR de salida extrae la etiqueta lee la cabecera IP y envía el paquete a su destino final.

Se ha utilizado una denominación para los diferentes tipos de LSR en un dominio MPLS, así tenemos:



P - Provider router

Estos equipos son los que forman el core MPLS, en ellos simplemente se implementa OSPF como IGP para que se comuniquen los equipos del core.

PE - Provider Edge

Estos equipos se encuentran en el borde o límite del dominio MPLS y son los que realizan la comunicación entre el mundo IP y el mundo MPLS, entre estos equipos de borde es necesario implementar BGP para establecer la conexión entre el EGP de cada PE.

CE - Customer Edge

Estos equipos se encuentran fuera del Dominio MPLS y son los equipos terminales para cada cliente final, el direccionamiento entre el PE y los CE puede ser RIP o EIGRP que vienen a ser el protocolo EGP del dominio MPLS, permitiéndose usar diferentes protocolos en los diferentes extremos de una misma conexión, es decir hay una doble redistribución, por ejemplo si los datos que ingresan con RIP por un PE se encapsulan y se des encapsulan al salir del core en IGRP.

RR - Route Reflector

Son equipos utilizados para distribuir tablas de enrutamiento y disminuir el número de conexiones. El uso de este elemento está previsto solo si el número de PE es mayor a 15.



En la figura 2.5 se muestran los componentes de una red IP/MPLS, y la forma en que están distribuidos.

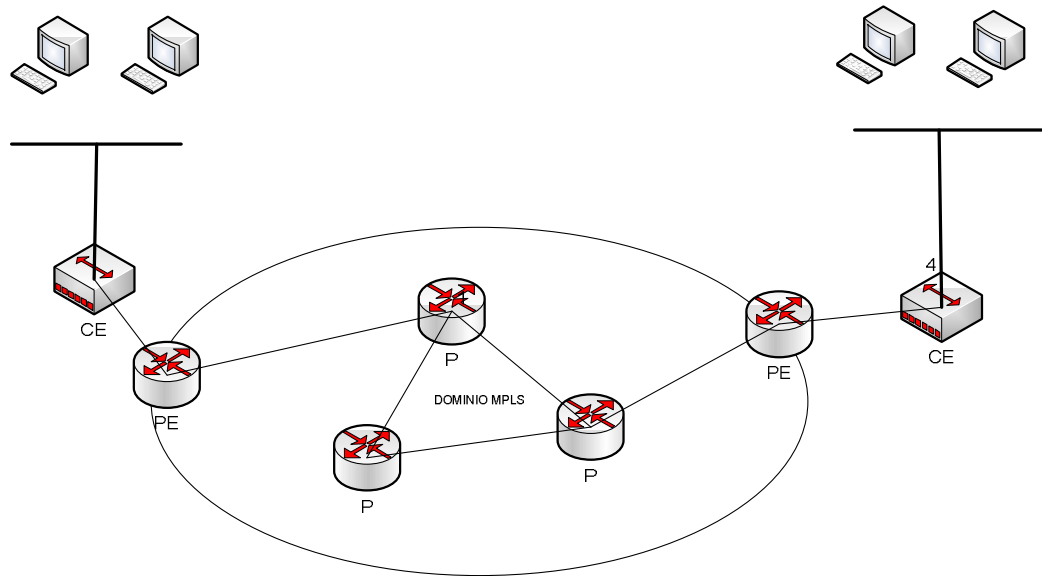


Figura 2.5 Componentes del dominio MPLS

Etiquetas

Las etiquetas son la base para MPLS. Un router genera una etiqueta por cada FEC que posea. Un router de núcleo o router Provider en la terminología MPLS intercambia tramas puramente basándose en etiquetas, y no accede a información IP de capa 3 refiriéndonos al modelo OSI, mientras que los PE según la función que estén realizando pueden o no acceder a la información IP.

Tabla TIB

Cada LSR posee una tabla TIB (Tag Information Base, o Base de información de etiquetas) de reenvíos para cada LSP, así cuando llega un paquete etiquetado el LSR indexa la tabla de saltos o TIB para determinar el siguiente salto. Siendo también función del



LSR de borde y específicamente de ingreso de borde determinar la FEC de cada paquete entrante no etiquetado.

Es importante aclarar que las etiquetas son de uso local únicamente. Cuando un conmutador recibe un paquete etiquetado, utiliza la información de esa etiqueta como un índice para buscar en su TIB para localizar una entrada igual. Cuando localiza un registro que se ajusta a la entrada recibida, sustituye esta información por una nueva etiqueta de salida y la reenvía por el interfaz asociado a la etiqueta entrante.

Tabla FIB

Cada conmutador en el core posee una Forwarding Information Base o FIB, que es una tabla que recopila la información de las Tablas TIB de cada conmutador de core, más las tablas que recibe de los demás conmutadores que pertenecen a la misma AS (Autoridad Administrativa) o Dominio MPLS, las rutas de estas tablas son los LSP

Conexiones de capa de enlace de datos

En la capa de enlace del modelo OSI o capa 2, MPLS nos permite crear enlaces transparentes para el usuario, para esto tenemos 2 tipos de tecnologías, en ninguna de las cuales el administrador de la red tiene que participar en el direccionamiento de capa 3 del cliente:



AToM

Conexión de punto a punto, simula que es una conexión directa, es decir un cable lógico, además AToM permite Interworking o flexibilidad de encapsulación que permite la interacción entre diferentes tecnologías como Frame Relay y Ethernet por ejemplo.

VPLS

Conexión de punto a multipunto, es una VPN de capa 2 avanzada, para su implementación requiere de tarjetas especiales: CIP, ES20, esto dependiendo del chasis de los routers.

Conexiones de capa de red

A nivel de capa de red o capa 3 MPLS permite la creación de vrf, en este tipo de conexiones el Administrador debe participar en el enrutamiento del cliente.

Podemos referirnos a una VRF o VPN Routing and Forwarding como una VPN-MPLS, que básicamente esta compuesta por una tabla de routing y una tabla de forwarding, el principal problema que solventan las VPN MPLS es el aislamiento del tráfico de diferentes clientes quienes son totalmente inconscientes del uso de una VPN MPLS ya que el tráfico se transmite de una manera totalmente transparente.

VRF



Una VRF (Encaminamiento y Reenvíos Virtuales - Virtual Routing and Forwarding) es una tecnología que permite la coexistencia de varias tablas de enrutamiento dentro del mismo router al mismo tiempo. Dado que las tablas de enrutamiento son independientes se puede usar el mismo direccionamiento IP para los clientes sin que exista conflicto. Las VRFs existen únicamente en los equipos PE que son los enrutadores de borde en un dominio MPLS, de donde decimos que una VRF se define entonces como una instancia de una tabla de enrutamiento, donde pueden existir más de una VRF en un router de borde o PE.

Las tablas FIB son utilizadas por los enrutadores para definir una VRF, en este caso se utiliza una tabla FIBs por VRF que se configure.

Los routers PE comunican la información de las VRFs que contienen entre sí, para lo cual se utiliza un protocolo de tipo BGP

Características importantes de una VRF:

Router Target (RT).- esta característica se utilice como el ID de la VRF

Router Distinguisher (RD).- permite que los usuarios puedan tener las mismas subredes. Cada router tiene ligado un RD lo cual lo identifica de manera única en el core de red.



2.3 Protocolos de Administración

2.3.1 SNMP Simple Network Management Protocol

Es un protocolo que forma parte de la familia de protocolos TCP/IP esta presente en la capa de aplicación y se utiliza para facilitar el intercambio de información de administración entre dispositivos de una misma red. SNMP surge para resolver los problemas de administración de redes TCP/IP, dado que el crecimiento apresurado y desmesurado de las redes de datos, ha hecho que la administración y gestión de las mismas se convierta en una labor intensa.

Arquitectura

La arquitectura de administración SNMP utilizan una estructura con estaciones terminales de usuario como los sistemas de computo u otros dispositivos de red, SNMP utiliza un protocolo que permite el envío de mensajes de información, al recibir estos mensajes las entidades de administración están configuradas para reaccionar ejecutando acciones como por ejemplo la notificación del suceso al administrador, etc.

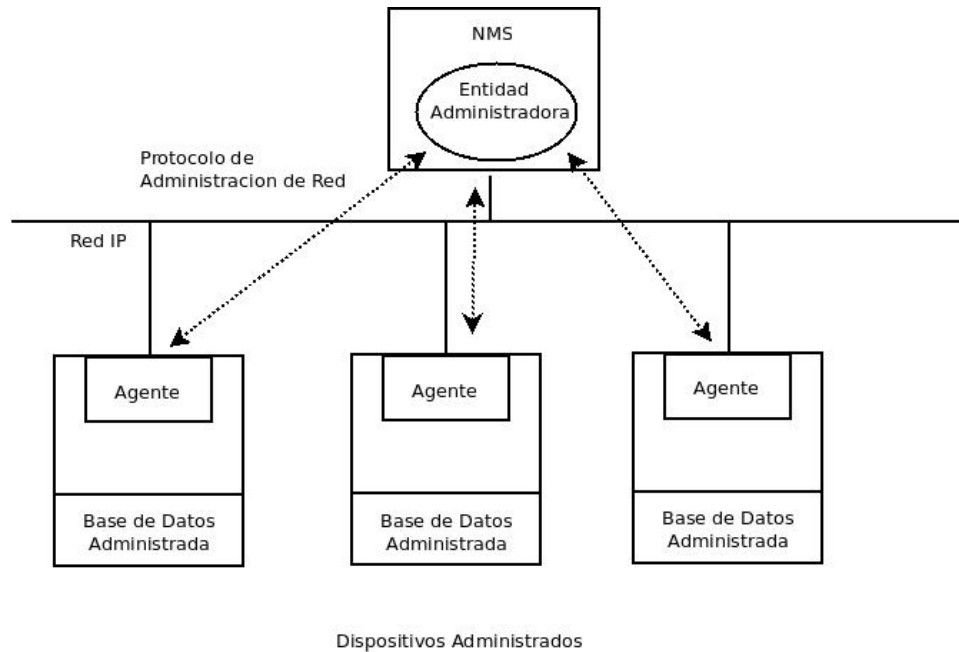


Figura2.6 Modelo de funcionamiento SNMP

Componentes

Una red administrada a través de SNMP consiste de tres componentes claves:

- Dispositivos administrados.- es un nodo de red entiéndase cualquier dispositivo como router switch, laptop, etc. que tiene un agente SNMP el cual recopila y guarda información del equipo en donde reside, dicha información la coloca a disposición de los NMSs o Sistemas Administradores de Red.
- Agentes.- es un modulo de software que se encuentra presente en los dispositivos de red de una red administrada, el agente



transforma la información que recopila del nodo en el que reside y la pasa a un formato compatible con el protocolo SNMP.

- Sistemas administradores de red (NMS's).- conocido también como Gestor, es una entidad que controla los dispositivos administrados y maneja los datos generados por los nodos o equipos controlados de la red generando información de administración.

En algunas definiciones se considera a la base de información que reside en cada equipo conocida como MIB como un componente de la arquitectura pero para este documento se mencionan los elementos clásicos de la arquitectura original considerados inicialmente.

Management Information Base - MIB

Una MIB o Base de Información de Administración es una colección de definiciones que brindan información de las propiedades de un dispositivo que se pueden gestionar mediante SNMP, dicha información está organizada de manera jerárquica.

Básicamente se puede ver a las MIBs como tablas donde se concentra toda la información de cierto dispositivo físico, así como las operaciones que están permitidas realizarse en el.

Gracias a esta estandarización independiente del fabricante una MIB y sus mecanismos de acceso, se puede controlar y supervisar de manera



centralizada en una red heterogénea formada por componentes de diferentes fabricantes.

Si para la supervisión de red se necesitan datos específicos de componente no estándar, se puede utilizar el llamado MIB privado descrito por el fabricante. De esta forma, también se pueden consultar valores que no cumplan con el estándar MIB. Los objetos MIB privados siempre se guardan dentro del directorio "Enterprise", que se explicara con más detalle mas adelante.

Una MIB esta compuesto de instancias de objeto que pueden ser:

- **Objetos Escalares** (o Variables Simples): tienen sólo una instancia asociada con cada objeto escalar, que se identifica por concatenar un valor 0 al OBJECT IDENTIFIER.
- **Objetos Columnares** (o Tablas): las instancias de estos objetos se identifican en una tabla por la cláusula INDEX, que se refiere a una fila en una tabla. (Fig. 8.6)
- **Tablas y Filas Conceptuales:** no tienen identificadores de instancias asociados.
- **Orden Lexicográfico:** los OBJECT IDENTIFIERs están ordenados en forma creciente en las MIBs SNMP.



Las MIBs están definidas por diferentes RFCs: RFC1212², RFC1213³, que definen las funcionalidades que proporcionan.

Actualmente se definen los siguientes estándares MIB:

- MIB2
- Bridge-MIB
- RMON-MIB
- MAU-MIB

Los NMS/ESM (Sistemas de Gestión) con capacidad de administración de red deben soportar los siguientes estándares MIB:

- RFC1213: MIB II
- RFC 2233: Interface MIB
- RFC1286, RFC1493: Bridge–MIB
- RFC1757: RMON–MIB

Para conocer el valor de una instancia de un objeto dentro de la base MIB, se necesita identificar la instancia, usando el OBJECT IDENTIFIER u OID como también es conocido

Object Identifier OID

Un Object Identifier se utiliza para referenciar los objetos de una MIB de manera única mediante una colección de números que lo distinguen

² Definiciones de MIB Concisa”, provee métodos para limpiar y remover las descripciones de objetos redundantes

³ Definición de MIB II.- Administración de Redes de Internet basadas en TCP/IP:
<http://www.faqs.org/rfcs/rfc1213.html>



frente a los demás objetos. Dicho identificador se denomina *Object Identifier* o abreviadamente *OID*

Un ejemplo de un objeto administrado es *atInput*, un objeto escalar, cuyo valor entero indica el número total de paquetes Apple Talk de entrada sobre una interfaz de un router.

El OID correspondiente, sería:

iso.identified.dod.internet.private.enterprise.cisco.temporary.AppleTalk.atInput = 1.3.6.1.4.1.9.3.3.1

En el siguiente grafico podemos ver el árbol del router y la ruta que nos guía el *OID*.

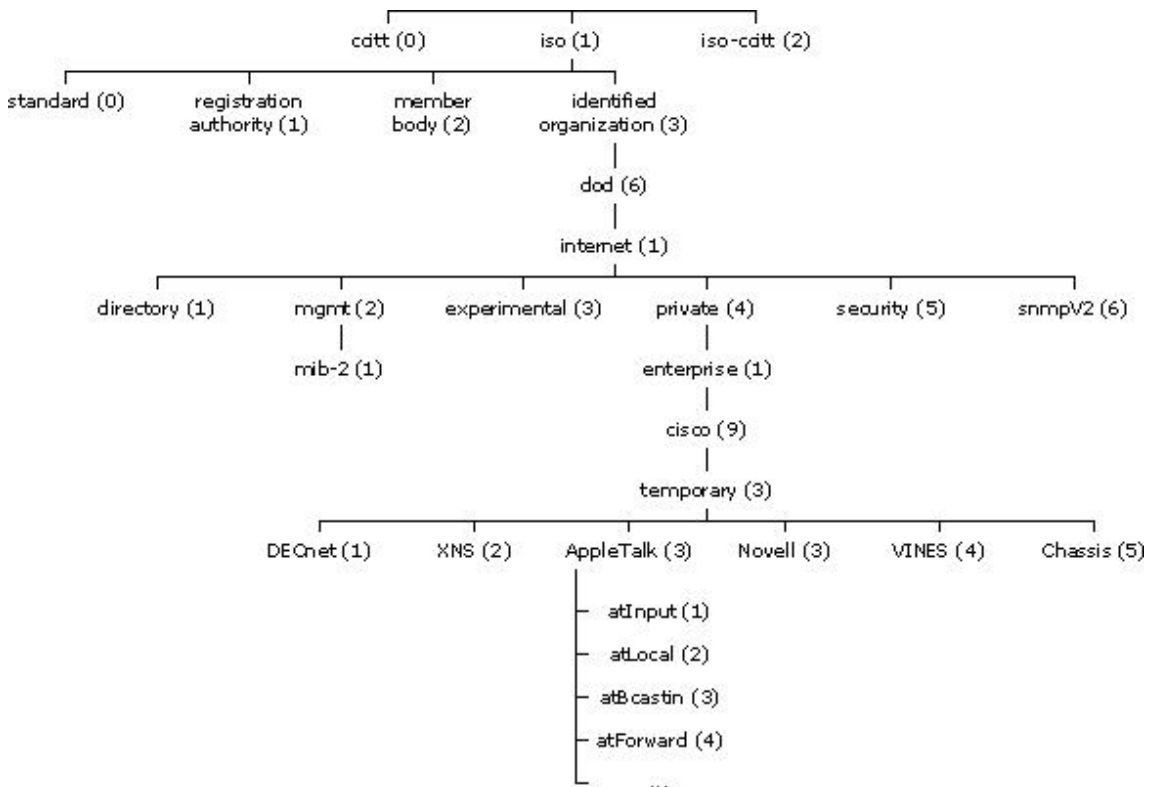


Figura 2.7 Ejemplo de árbol MIB de OID



Los objetos a gestionar están ordenados en una jerarquía que permiten asignar a cada objeto un identificador único Object Identifier (OID) que es una secuencia de números que forman parte de ese árbol de profundidad arbitraria en el que el nodo raíz está sin etiquetar y posee al menos tres nodos hijo administrados por entidades supranacionales como el International Telegraph and Telephone Consultative Committee (CCITT), y la International Standards Organization (ISO).

Los OIDs son asignados por el IANA (Agencia de Asignación de Números de Internet) de forma similar a como se hace para las delegación de dominios en Internet, de tal forma que se acostumbra a delegar, para cada fabricante, una rama de OIDs a partir del nodo Enterprise.

Es por eso que los OID de los objetos en la parte superior del árbol pertenecen a organizaciones estándares y los OID de los objetos ubicados en la parte inferior del árbol son colocados por organizaciones asociadas.

Para los vendedores pueden incluso definir ramas privadas que incluyen los objetos administrados para sus productos en particular. Las MIB's que no han sido estandarizadas típicamente están localizadas en la rama experimental.

La selección de los OIDs puede provocar problemas si dos dispositivos diferentes llegan a tener OIDs idénticos. Al gestionar mediante SNMP se puede solucionar esto estandarizando la información proporcionada



por los diferentes MIBs, esta es la tarea de SMI (Structure of Management Information) que especifica un conjunto de reglas para la nomenclatura de los diferentes objetos gestionados.

SMI Structure of Management Information

Para que un objeto sea definido en una MIB deben seguir un determinado conjunto de reglas como las establecidas por la Estructura de Información de Administración (SMI). Es decir el SMI describe el modelo de información de un objeto que será incluido en la MIB. Una SMI esta dividida en tres ámbitos:

- **Module definitions.-** sirve para describir información de los módulos o conjuntos de objetos relacionados gestionados en una MIB, se usa para llevar consistentemente la semántica de un módulo de información.
- **Object definitions.-** se utiliza para describir los objetos manejados, y para llevar consistentemente la semántica de un objeto
- **Notification definitions.-** también conocido como traps las cuales son utilizadas cuando se tiene que transmitir información que no son solicitada a los NMSs, es decir lleva consistentemente la sintaxis de una notificación. Las notificaciones tipo Trap serán detalladas mas adelante.

Versiones de SNMP



Todas las versiones de SNMP (SNMPv1, SNMPv2 y SNMPv3), tienen la misma estructura básica y los mismos componentes y además de eso conservan las bases de la arquitectura original.

Los Estándares SNMP se ha definido en una serie de documentos RFC propuestos por la IETF una lista de RFCs para SNMPv1, SNMPv2, SNMPv3. La IETF actualmente recomienda el uso del protocolo SNMP v3.

SNMPv1

SNMP Versión 1 es la implementación inicial del protocolo de gestión de red y consistía de los siguientes RFCs:

- 1155 (sintaxis y semántica para definir objetos para administración de red - SMI),
- 1157 (protocolo de administración para acceder a los objetos, monitorearlos y controlarlos - SNMP)
- 1212 (lineamientos para definir nuevos módulos sin generar redundancia – MIB Concisa).

Luego, se agregó el RFC 1213 que provee las definiciones de un conjunto central de objetos – MIB II. Una clara desventaja de SNMPv1 es la seguridad, ya que para los métodos de autenticación se utiliza un esquema de dos palabras clave llamadas communities de tipo string que indican la comunidad a la que pertenece el nodo administrado donde dichas palabras son



transmitidos en formato de texto plano fácil de interceptar e interpretar.

- La clave pública permite a los gestores realizar peticiones de valores de variables
- La clave privada permite realizar peticiones de escritura

SNMPv1 provee los siguientes tipos de acceso a la información de gestión:

GESTOR-AGENTE, pregunta-respuesta.

AGENTE-GESTOR, sin confirmación de entrega

SNMPv2

Surge ante la necesidad de cubrir algunas de las deficiencias del SNMP original (SNMPv1). SNMPv2 incorpora nuevas características en cuanto al desempeño, seguridad y confidencialidad como por ejemplo SNMPv2 Trap que utiliza un diferente y mejor formato de mensaje que SNMPv1 trap. Sin embargo no todo fue para mejorar, las nuevas características implementadas en cuanto a seguridad produjeron demasiada complejidad y afectaron el desempeño del protocolo por lo que no fueron aceptadas, de ahí que se desarrollo la versión SNMv2c sin dichas medidas de seguridad y se empezó con la propuesta de la versión 3 del protocolo.

Además se definen nuevas operaciones: GetBulk e Inform. La operación GetBulk es utilizada para recuperar grandes cantidades de datos de los agentes y la operación Inform permite



a un NMS enviar información de traps a otros NMS y recibir respuesta de tales operaciones.

SNMPv2c provee tres tipos de acceso a la información de gestión:

GESTOR-AGENTE, pregunta-respuesta.

GESTOR-GESTOR, pregunta-respuesta (nuevo con respecto SNMPv1).

AGENTE-GESTOR, sin confirmar

Las PDU de SNMPv2 van encapsuladas en un mensaje como en SNMPv1 así como las consideraciones hechas sobre los nombres de comunidad y los perfiles de comunidad.

SNMPv3

La tercera versión de SNMP (Simple Network Management Protocol), fue creada a partir de las versiones anteriores, SNMPv1 y SNMPv2c.

SNMPv3 conserva los principios arquitectónicos de las versiones anteriores y basándose sobre éstos incorpora mejoras de seguridad y de administración en la arquitectura. Y ofrece nuevos beneficios a las redes TCP/IP ya que es en este nivel donde es probable que se pueda efectuar la captura de algún tipo de tráfico que circula por la red, falsificando su dirección IP, originando con esto datagramas no confiables, para solventar este



inconvenientes SNMPv3, ha mejorado los procesos de identificación de usuarios (Autenticación) de la red.

Los servicios de seguridad que ofrece el modelo de SNMPv3 son los siguientes:

- Integridad de la Data.- Previene la manipulación de los datos por entes externos sin privilegios de acceso a la data.
- Autenticación del origen de los datos.- verifica la identidad del usuario que solicita información.
- Confidencialidad de los datos.- Garantiza que nadie acceda a los datos ya sea para lectura o escritura.

La seguridad está dividida en tres módulos:

- Módulo de Autenticación.- modulo encargado de la Autenticación y verificación del origen de los datos.
- Módulo de Tiempo (Timeliness).- Brinda protección contra el retraso o repetición del mensaje. Se ejecuta solo si el proceso de autenticación a terminado.
- Módulo de Reserva.- Protege los datos y garantiza la confidencialidad de los mismos una vez el mensaje haya sido autenticado.

Es importante indicar que el protocolo SNMPv3 proporciona autenticación mediante un modelo orientado a usuario o *User-based Security Model (USM)* que utiliza algoritmos HMAC-MD5-



96 y HMAC-SHA-96 para autenticación y garantiza además la privacidad de las comunicaciones mediante CBC-DES

En RFC 2571 se especifica más detalladamente la arquitectura de SNMPv3.

Operaciones Funcionales

SNMP es un protocolo de request-and-response (petición y respuesta), de donde las operaciones básicas que se llevan a cabo son categorizadas como las siguientes:

- **Recolección de datos.-** El gestor o NMS envía un requerimiento a un agente que responde al requisito con los datos correspondientes, en este caso se utilizan las siguientes operaciones:
 - **GET:** La operación GET es una petición enviada por el gestor al agente el cual devuelve uno o más valores de acuerdo al requerimiento.
 - **GETNEXT:** esta operación es similar a la operación GET, la diferencia radica en que GETNEXT recopila el valor del siguiente OID en el árbol.
 - **GETBULK:** La operación GETBULK es usada para la recolección de grandes volúmenes de datos provenientes de tablas de gran tamaño.



- **Alteración de variables.-** este tipo de operaciones son utilizadas por el gestor cuando quiere realizar cambios en las variables de un nodo de red.
 - **SET:** esta operación cambia los valores de las variables de los dispositivos de red.
- **Recepción de mensajes no solicitados.-**el uso mas practico de estos mensajes se da por parte de los agentes que envían información a lo gestores, información que no ha sido solicitada y que informa comúnmente de problemas en el dispositivo de red
 - **TRAP:** es la operación donde el agente envía mensajes no solicitados que son receptados por el NMS

Mensajes SNMP

Los mensajes mas comúnmente utilizados en una red gestionada en base al protocolo SNMP son lo siguientes:

- **GetRequest** .- Es usado por el NMS cuando quiere información del agente.
- **GetNextRequest** .- Este mensaje se usa para recorrer una tabla de objetos. Si ya se ha usado el mensaje GetRequest, después se usa GetNextRequest para repetir la operación con el siguiente objeto de la tabla.
- **SetRequest** .- Usado por el NMS cuando solicita al agente modificar valores de objetos. El NMS envía al agente una lista de los objetos con los valores a ser cambiados.



- **GetResponse.-** mensaje que lo usa un agente cuando responde un mensaje GetRequest, GetNextRequest, o SetRequest.
- **GetBulkRequest.-** Un NMS con la versión 2 ó 3 de SNMP, se utiliza para transmisiones largas de datos, recuperación de largas tablas, etc. Es parecido a GetNextRequest de la versión 1, pero GetBulkRequest es más rápido y eficiente, por que con un solo mensaje solicita toda la tabla por ejemplo.
- **InformRequest .-** este tipo de mensajes son notificaciones que requieren confirmación de su recepción, generalmente se dan para el intercambio de información entre NMSs (con las mismas características) que utilizan la versión 2 ó 3 del protocolo SNMP para notificar información sobre objetos administrados.
- **Traps.-** estas notificaciones son menos pesados ya que no requieren de confirmación del receptor cuando este haya recibido el trap. Por tal razón los traps se prefieren ante las notificaciones de tipo inform, ya que consumen menos recursos de la red. Un trap es generado por el agente para reportar ciertas condiciones y cambios de estado al NMS.

Comunicación entre el agente y el NMS

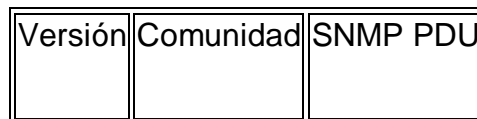
Cuando un agente se asocia con un conjunto de agentes en una red con uno o más gestores NMS, ha este par se conoce como comunidad. Cada comunidad tiene un identificador conocido como “nombre de comunidad”.



Un Mensaje SNMP consiste de un Identificador de Versión, un Nombre de Comunidad SNMP y una PDU SNMP. Hay que tomar en consideración que los mensajes intercambiados entre una NMS y los agentes son independientes unos de otros.

La PDU o Protocol Data Units permiten a los gestores interactuar a través de la red con los agentes que se encuentran en los dispositivos, para lo que se utiliza los puertos 161 para mensajes SNMP y 162 para mensajes SNMP de tipo Trap, esto en el protocolo UDP sin conexión ya que un transporte orientado a la conexión agregaría complejidad. Por tanto las PDU son encapsuladas dentro de paquetes UDP (User Datagram Protocol).

Formato de los paquetes SNMP .- El formato de los paquetes SNMP para consultas y respuestas es el siguiente:



Descripción de los campos:

- Versión: versión de protocolo
- Comunidad: es el nombre clave que se usa para la autenticación, en este caso hay de 2 tipos:
 - Comunidad de lectura "public"
 - Comunidad de escritura "private";
- SNMP PDU: este campo depende del tipo de operación que se realice, para los mensajes: GetRequest, GetNextRequest,



SetRequest y GetResponse, se tiene la siguiente estructura en el campo SNMP PDU:

Tipo	Identificador	Estado de error	Índice de error	Enlazado de variables

Descripción de los campos:

- Identificador: utilizado por el NMS y el agente para enviar e identificar la solicitudes y respuestas.
- Estado de error: puede tener los siguientes valores:
 - 0: No hay error;
 - 1: Demasiado grande;
 - 2: No existe esa variable;
 - 3: Valor incorrecto;
 - 4: El valor es de solo lectura;
 - 5: Error genérico.
- Índice de error: (cuando "estado de error" es diferente a 0) posee el objetivo que proporcionar información del problema.
- Para los mensajes GetResponse en consultas siempre tendrá un valor de cero.
- Enlazado de variables: son nombres de variables con sus valores correspondientes.



CAPITULO III

DISEÑO E IMPLEMENTACION

DEL PROTOTIPO



3 CAPITULO III: DISEÑO E IMPLEMENTACION DEL PROTOTIPO

3.1 ANALISIS

3.1.1 Requerimientos

Situación Actual

La Dirección de Telecomunicaciones, encargada de las funciones junto con su similar comercial CentroNet en calidad de prestación de servicios como portador pretende realizar una gestión de redes que brinde un servicio eficiente para sus clientes con tecnologías de punta llevando a la vez una administración adecuada de los elementos involucrados en el área operativa de la red.

Visión

“Comercializar los servicios de Telecomunicaciones que ofrece la Empresa Eléctrica Regional Centrosur C.A., satisfaciendo las necesidades de los clientes con un servicio de calidad, a precios competitivos y con amplia cobertura, así como generando rentabilidad social y sostenimiento económico”.

Misión

“Consolidarnos como marca líder en innovación del servicio de telecomunicaciones, a través de un proceso de mejoramiento continuo que permita brindar soluciones globales, tanto al sector residencial como empresarial, a través de un servicio personalizado para cubrir las expectativas de todos y cada uno de nuestros clientes”.



Con la implementación de los protocolos de red como MPLS la DiTel se coloca en la vanguardia de los modelos de administración de red que les permite llevar una cartera importante de clientes tanto a nivel corporativos como residencial que poseen conexiones de internet con diferentes características derivadas de la gama de servicios que ofrece la empresa. Toda la gestión de configuraciones necesaria para levantar los servicios genera una cantidad de información diaria que al momento no cuenta con un repositorio central.

En la actualidad la red MPLS de centrosur cuenta con alrededor de 30 equipos solo en el dominio mpls en diferentes jerarquías dentro del dominio mpls que cumplen variadas funciones pero que cooperan en el desempeño general de la red, dicho equipos no cuentan con un sistema centralizado de respaldos para las configuraciones que corren en los sistemas operativos de los mismos.

Al momento se tiene personal asignado en cada área operativa, cada operador es responsable de las tareas que desempeña y así como la gestión de la información que utiliza en sus tareas diaras en la red. Esto hace que se genere una dependencia del personal que no es buena.

Servicios prestados por el operador

Internet Residencial

El servicio de Internet residencial se proporciona en base a zonas de cobertura wifi en ciertos sectores de la ciudad de Cuenca. A nivel de



Universidad de Cuenca

internet residencial CentroNET ofrece varios planes para los usuarios a diferentes costos.

A nivel técnico la compresión del servicio es de 8:1 y 6:1 para planes residenciales

Internet Corporativo

La Empresa Eléctrica ofrece también el servicio de internet corporativo para empresas con el uso de tecnología inalámbrica y de fibra óptica.

Los enlaces de nivel corporativo que se realizan con fibra, tanto como los implementados con antenas inalámbricas son gestionados con el core IP/MPLS de Centrosur.

Actualmente existen dos niveles de compresión para enlaces de tipo corporativo

Compresión 2:1

Compresión 1:1

Esto con diferentes anchos de banda

Entrevistas con el personal del área de administración

El Personal de la Dirección de Telecomunicaciones a cargo del proyecto y con el que se trabajo realizando entrevistas para la captura de requerimientos esta integrado por el Ingeniero Diego Unkuch que se desempeña como el Administrador de Red Centrosur IP/MPLS,



encargado de gestionar las configuraciones en los equipos de Red y llevar registros de información de las configuraciones que se realizan.

De igual manera para la captura de requerimientos de conto con el apoyo del Ingeniero David Regalado que ocupa el cargo de Soporte para los clientes de CentroNet, a cargo de las tareas de monitoreo así como la colaboración en tareas de mantenimiento y configuración de la red conjuntamente con el ingeniero Unkuch

De las entrevistas realizadas al personal del área operativa de la Dirección de Telecomunicaciones antes mencionado se ha recopilado la siguiente información que describe los procesos de gestión de configuración efectuados en la red centrosur IP/MPLS, se ha clasificado esta información en temas independientes a fin de enfocar el desarrollo de estas soluciones de una manera mas puntual.

Respaldos de Configuración

Actualmente no se cuenta con una solución de respaldos de las configuraciones de los equipos que forman parte de la red Centrosur IP/MPLS, el proceso que se efectúa es ingresar a los equipos mediante programas de conexión remota como putty que permiten un ingreso vía telnet a las terminal de configuración de los equipos, una vez ingresados ahí se copia la configuración que corre en el equipo manualmente a archivos de texto plano que son almacenados de manera local en los equipos personales de los operadores de Red con nombres descriptivos de la configuración que ha sido respaldada.



Proceso de configuración

Las configuraciones en los equipos de la red que involucran la creación de enlaces para los clientes tanto corporativos como residenciales son realizadas de manera manual por el Ing Diego Unkuch accediendo a los equipos con programas de conexión remota como putty, el Ingeniero gestiona la información generada en estos procesos tanto en documentos del paquete office 2003 de Microsoft como Excel para el registro de direcciones IP aplicadas en los puertos de los equipos como direcciones ip aplicadas a las vlans en los switch o conmutador multicapa de la red, también en documentos de Visio para la generación de diagramas de red que permitan una visión de la distribución física de los equipos. Además se utilizan documentos de google docs de su cuenta personal donde esta registrada información de direccionamiento IP que es requerida por el personal de Soporte para sus tareas de monitoreo, estos documentos están publicados sin restricción de modo que el personal de soporte puede acceder para visualizar la información lo que afecta los niveles de seguridad de la red ya que cualquier persona que tenga el link de acceso podrá visualizar dicha información

Los datos que relacionan información de configuración de equipos como vrf con los clientes para quienes se realizo dicha configuración se guarda en archivos de Excel del paquete office y que se almacenan en el computador personal del Ingeniero Diego Unkuch.

Las configuraciones requieren niveles de conocimiento de networking y del protocolo MPLS específicos para este tipo de redes que no pueden



ser ejecutados por parte del personal de soporte quienes tienen conocimiento del funcionamiento de la red y más no el conocimiento técnico en cuanto a comandos de configuración del sistema operativo IOS de Cisco necesarios para ejecutar estas tareas.

El tiempo estimado por configuración varía de acuerdo a las tareas que se están ejecutando. Sin embargo se estima que el tiempo mínimo requerido para ingresar al equipo, efectuar una configuración de tiempo estimado medio y registrar la información de dicha configuración toma un estimado de 20 a 30 minutos. Sin tomar en cuenta que se debe contar con la disponibilidad de la persona que tiene el conocimiento para efectuar la tarea. Todo esto provoca que se dependa de personas más que del puesto que ocupan lo que pone en riesgo la gestión de estos procesos en el caso de existir ausencia de los involucrados. Hay que tomar en cuenta que el tiempo requerido para cada tarea ejecutada en los equipos, retrasa toda la cadena de procesos que involucra la prestación de servicios al cliente final y no brinda una fuente de información integrada.

Los procesos de configuración requieren la generación de subredes las cuales son calculadas mentalmente o con ayuda de calculadoras IP en Internet, después de aplicar las direcciones IP de estas subredes ya sea en VLANs o puertos en los equipos la información de las subredes se guarda como se mencionó anteriormente en archivos de Office y en un documento de Google Docs publicado a la web para que pueda ser visualizado por el personal de soporte.



3.1.2 Análisis y estudio de la Red Centrosur IP/MPLS

La empresa Eléctrica Regional Centro Sur que presta servicios de telecomunicaciones a través de su departamento de Dirección de Telecomunicaciones implemento una red IP/MPLS para la cual a continuación se detalla los diagramas en sus diferentes niveles.

Diagrama de Interconexión ISP

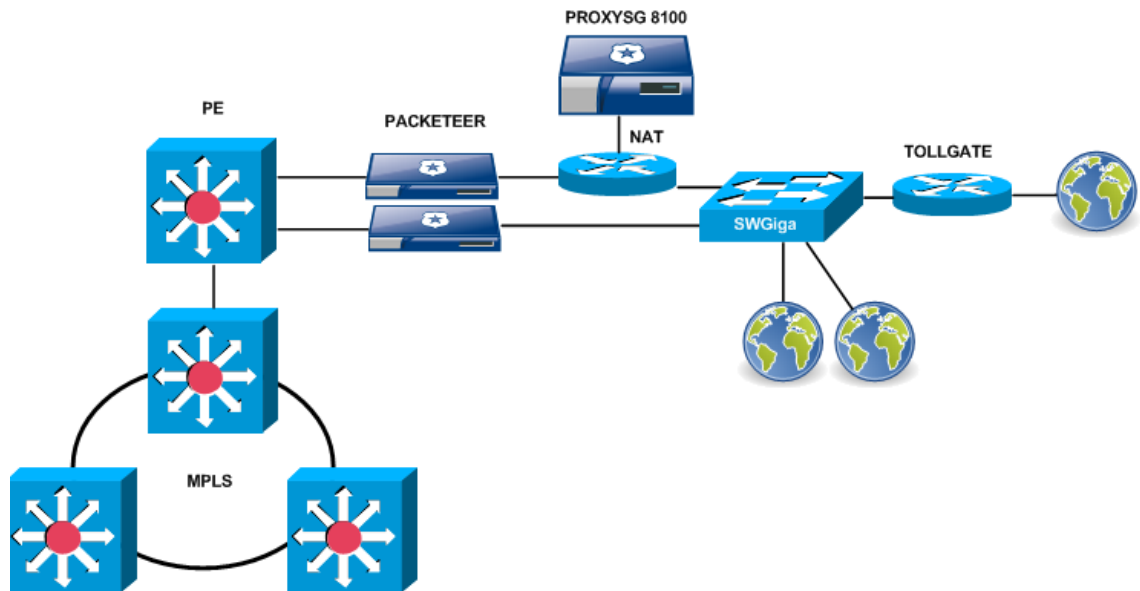


Figura 2.8 Diagrama de interconexión ISP de la red Centrosur Ip/MPLS

Core MPLS

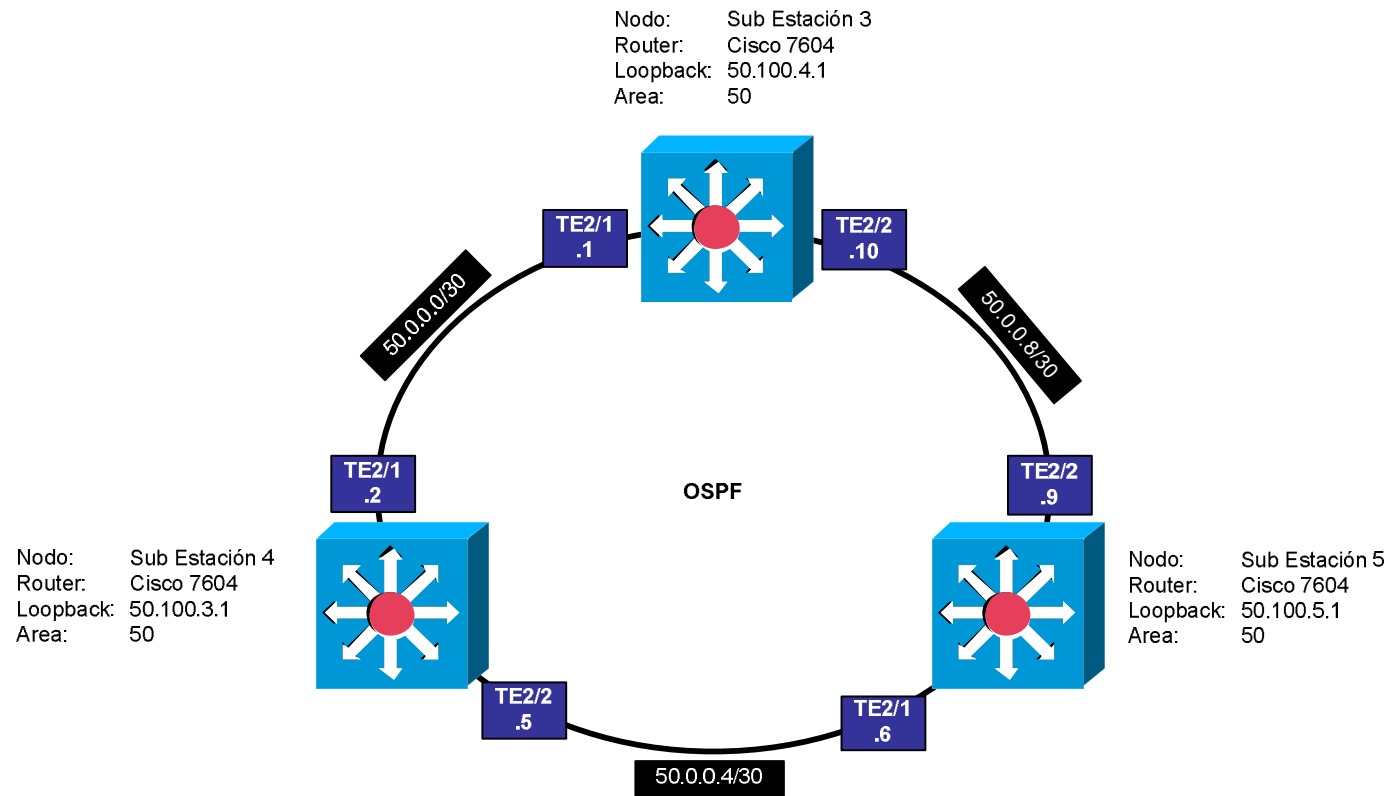


Figura 2.9 DIAGRAMA DE CORE DE LA RED Centrosur Ip/MPLS



Distribución

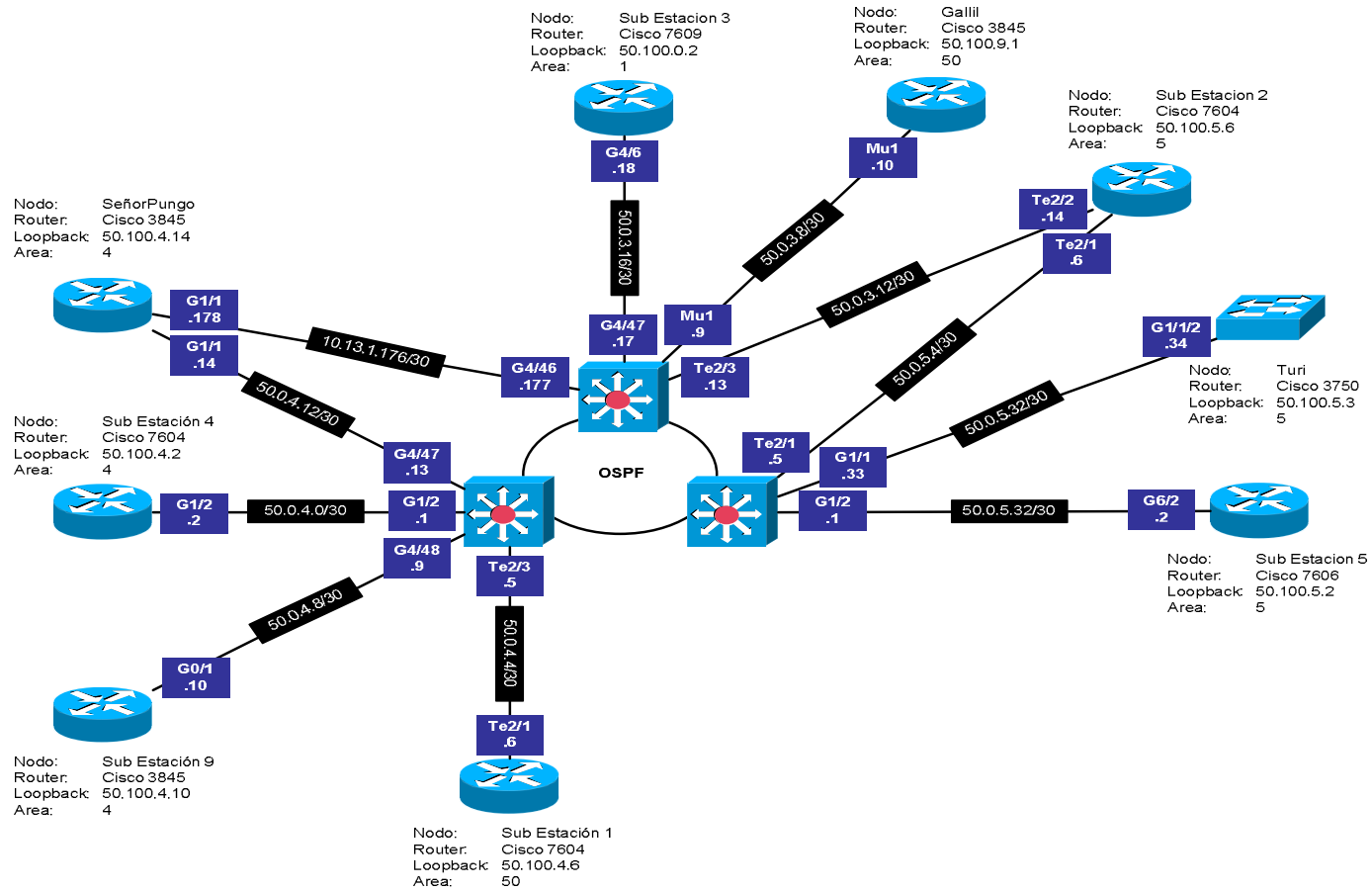


Figura 2.10 Diagrama de distribución de la red Centrosur Ip/MPLS



Acceso

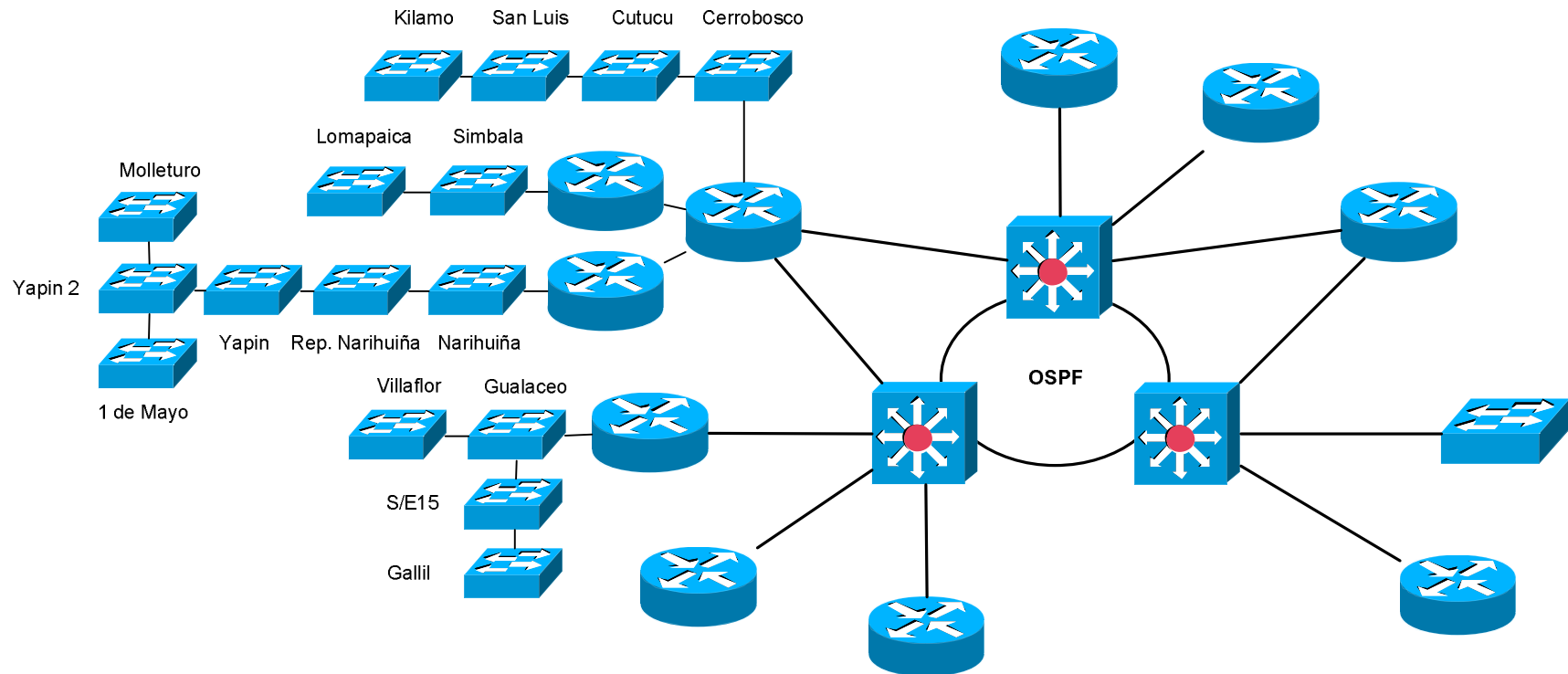


Figura 2.13.1 Diagrama de acceso de la red Centrosur Ip/MPLS

Diagrama Interconexión ISP

El Core MPLS se interconecta a través de un router de borde o Provider Edge mediante un enlace redundante conectado a dos equipos packeteer con un Switch Giga a través de un equipo ProxySG 8100 que realiza la tarea de NAT con tres salidas internacionales.

A continuación se listan jerárquicamente los elementos incluidos en el grafico de la red Centrosur IP-MPLS.

Core MPLS

La red IP/MPLS consta de 3 dispositivos Provider o P los cuales conforman el core del dominio MPLS, en tal fin se utilizan equipos 7604 Cisco Routers denominados como Nodos, los cuales están listados y detallados a continuación.

Sitio	Función	Denominación	Equipo	Numero de PEs
Sub Estación 3	Router P	P_SE 3	Cisco 7604	3
Sub Estación 4	Router P	P_SE 4	Cisco 7604	4
Sub Estación 5	Router P	P_SE 5	Cisco 7604	3



Los equipos del core MPLS se encuentran interconectados a través de fibra formando una anillo que tiene una capacidad de 10GB. Por conveniencia se ha denominado a cada uno como Nodo 3, Nodo 4 y Nodo 5 respectivamente dependiendo de la subestación donde se encuentran físicamente.

Equipos de Distribución

Algunos de los equipos PE tienen una conexión con dos diferentes equipos Provider o P para brindar redundancia y respaldo en caso de que exista caída de un enlace.

En los routers de borde o Provider Edge PE se utilizan varios modelos de equipos cisco dependiendo de la zona a cubrir, el nodo al cual esta conectado y el tráfico que tenga que gestionar.

La siguiente clasificación esta presentada de acuerdo al nodo al que están conectados.

Nodo 4

Nodo	Función	Denominación	Equipo	Area
Sr Pungo	PE	PE_SRPUNGO	Cisco 3845	4
Sub Estación 4	PE	PE_SE	Cisco 7604	4
Sub Estación 9	PE	PE_SE9	Cisco 3845	4



Sub	PE	PE_SE1	Cisco	50
Estación 1			7604	

Nodo 5

Nombre	Función	Denominación	Equipo	Area
Sub	PE	PE_SE5	Cisco	5
Estación 5			7606	
Turi	PE	PE_TURI	Cisco	5
			3750	
Sub	PE	PE_SE2	Cisco	5
Estación 2			7604	

Nodo 3

Nombre	Función	Denominación	Equipo	Area
Sub	PE	PE_SE3	Cisco	1
Estación 3			7609	
Gallil	PE	PE_GALLIL	Cisco	50
			3845	
Sub	PE	PE_SE2	Cisco	5
Estación 2			7604	



Acceso

Los equipos para el acceso son en su mayoría switch 3com o cisco donde se configuran VLAN que replican los canales de VRFs creados en los equipos de dominio MPLS. Como se observa en la figura anterior se forma un bridge con ayuda de los switch para extender el alcance realizando filtros de vlan en los equipos.

Equipos CE

Los equipos utilizados para desempeñarse como Customer Edge son de varias tecnologías como inalámbricas en el caso del internet residencial, y en su gran mayoría routers para los servicios de internet corporativo y enlaces de datos.

Características de la Red IP/MPLS

Se definirán ciertos parámetros que norman el formato utilizado para clasificar y definir las diferentes entidades configurables. Dichos parámetros se nombran a continuación:

Códigos

Sistema Autónomo (SA):

28025 SA

Identificadores (ID):

10 Transmisión de datos

15 Internet corporativo



Universidad de Cuenca

16	internet residencial
25	Gestión de tecnología
50	Gestión NOC
11	Central Services

Servicio:

TD	Transmisión de datos
IC	Internet Corporativo
IR	Internet Residencial

Otros

#contrato Numero de Contrato de servicio del Cliente.

Nomenclaturas CS

El formato usado para nombrar una Central Services o Vrf Matriz, es el siguiente:

CS "Servicio" "#contrato"

Para los valores de route distinguisher (RD) y route target (RT) de Central Services, se usa el siguiente formato:

SA: 11 "Servicio" "#particular"

La Nomenclatura usada para definir el nombre de una VRF en el dominio MPLS son los siguientes:



Universidad de Cuenca

Para los valores de route distinguisher (RD) y route target (RT) de una VRF, se usa el siguiente formato:

SA : ID : XXXXXXXX -> XX (los 2 primeros) son el ID los 5 siguientes son un código

Protocolos

En la red Centrosur IP/MPLS se utiliza ospf como IGP que permite la conectividad entre los equipos que forman parte del núcleo.

En los equipos PE se utiliza un protocolo para el intercambio de información entre sistemas autónomos BGP para que exista interconectividad entre los PE, el modelo que se utiliza en dominios mpls extensos es un equipo denominado Route Reflector o RR, que es un Provider Edge dedicado a esta función y al cual apuntan todos los PE, el RR se encarga de gestionar la comunicación entre PEs lo que disminuye significativamente la carga de tráfico BGP en el core MPLS, este modelo se utiliza como se menciona en dominios MPLS extensos con un número mayor de 15 PEs. Este no es el caso de la red Centrosur IP/MPLS, donde BGP se aplica en cada equipo apuntado a cada PE dentro del dominio al cual quiere tener acceso.

Como protocolo IGP se utiliza RIP para establecer la conexión entre los equipos que cumplen la función PE y CE. En la mayoría de los casos se opta por rutas estáticas ya que la redistribución del tráfico RIP y BGP conlleva una carga adicional para la red que no se presenta con el uso de rutas estáticas.



3.1.3 Breve descripción de los equipos de la Red MPLS

Equipos

Cisco 7600 Series



Figura 2.12 cisco 7600 series

La serie 7600 presenta un alto desempeño de forma que proporciona alta disponibilidad en entornos MPLS, tanto en servicios de Provider Edge como Provider en sus diferentes versiones, Centrosur ha seleccionado para las diferentes funciones que desempeñan los router de la serie 7600 en sus versiones Cisco 7609/7604/7606, disponiéndolos de acuerdo a la carga que gestionan. Todos los equipos de la serie 7600 fueron fabricado bajo las normas de Construcción de Equipos de Red (NEBS) Nivel 3 de cumplimiento. Tanto la versión de chasis **7609**, **7604** y **7606** admiten una amplia gama de prestación de servicios en cuanto a video IP y triple-play (voz, vídeo y datos) en la versión 7609, todas las versiones son aptas para la implementación tanto de redes WAN como MAN, poseen fuentes de alimentación redundantes, y tiene capacidad para tarjetas extensibles desde Fast Ethernet, Gigabit Ethernet y 10 Gigabit Ethernet. En cuanto a los módulos de Servicios, se



incluyen módulos de seguridad IP (IPsec), denegación de servicio distribuido, sistemas de detección de intrusos, análisis de redes, etc.



Figura 2.13 7606

Entre los datos mas importantes a destacar se ha resumido la siguiente tabla.

Modelo	Ranuras	Tasa de Transmisión	Rendimiento	MTBF	Poder	Peso	Dimensiones (H x W x D)
7609	9 RU	400 Mpps	720Gbps	7 años	208-240 VAC (recomendado)	Peso: 121 libras (54,9 kg, chasis solamente), 270 libras (122,5 kg; configuración completa)	93,3 x 43,1 x 53,3 cm
7606	7 RU	240 Mpps	480 Gbps	7 años	208 a 240 VAC	37,2 libras (16,88 kg)	30.98 x 43.81 x 54.61 cm
7604	5 RU	144 Mpps	320 Gbps	7 años	110 a 240 VAC	40 libras	22,225 x 44,45 x 55,245



							cm
--	--	--	--	--	--	--	----



Figura 2.13.2 7606

Cisco 3800 Series

El router Cisco de la serie 3800 en su versión 3845, utilizado en la red centrosur IP/MPLS en calidad de PE, proporciona concurrencia en la prestación de servicios tales como seguridad y voz tanto analógica y digital en llamadas, permite el soporte de puertos GE y de fibra. Con soporte de hasta 2500 túneles VPN con el módulo AIM-HP11-PLUS. Servicios como Antivirus defense Support mediante Network Admission Control (NAC), Intrusion Prevention, Cisco IOS Firewall support, etc.



Figura 2.15 3845



Universidad de Cuenca

La versión 3845 posee unas dimensiones 5.25 x 17.25 x 16 in. Considerando (H x W x D), un peso mínimo de 45 lb, Una especificación de poder de 100-240 VAC

Cisco 3700 Series

Entre algunas de las características de la serie 3700 de cisco se incluye soporte de calidad de servicio, limitación de velocidad, listas de control de acceso (ACL), Open Shortest Path First (OSPF) para configuración de enrutamiento, y la funcionalidad IPv6. Tiene un soporte de IOS mínimo de Cisco IOS Release 12.2(25)FZ or Cisco IOS Release 12.2(35)SE.



Figura 2.16 3750

Esta serie de equipos permite la configuración de Cisco StackWise que es una arquitectura de apilamiento optimizada para Gigabit Ethernet con capacidad de hasta 32 Gbps de interconexión, convirtiéndolo en un sistema de conmutación unificado altamente resistente. La tecnología Cisco StackWise une a un máximo de nueve interruptores individuales en una única unidad lógica. La pila se comporta como una unidad de conmutación única que es administrada por un interruptor general, elegidos de uno de los interruptores miembros. El interruptor principal automáticamente crea y actualiza todas las tablas de conmutación y



Universidad de Cuenca

enrutamiento. Siendo la configuración automática de nuevas unidades a la pila.

La Empresa Electrica en su red Centrosur IP/MPLS posee estos equipos en las configuraciones de:

Cisco Catalyst 3750-48TS-48 Ethernet 10/100 y cuatro puertos SFP

Cisco Catalyst 3750G-24T-24 Ethernet 10/100/1000 puertos



Figura 2.17 pila cisco 3700

La imagen IOS Base presenta características como calidad de servicio (QoS), listas de control de acceso (ACL), enrutamiento estático, Routing Information Protocol (RIP) y enrutamiento EIGRP, IPv6 y routing multicast.



3.1.4 Selección de Herramientas de Software Libre

Análisis

Para el presente proyecto se ha propuesto el uso e integración únicamente de herramientas de software libre que permitan el desarrollo de una aplicación con las características funcionales requeridas para un NMS.

En vista de las necesidades y requerimientos que el sistema debe cumplir se ha considerado hacer la aplicación en una plataforma web con una interfaz RIA o Rich Internet Application, mediante el uso del lenguaje Action Script y ciertos Frameworks que faciliten el desarrollo. Por temas de compatibilidad y de un futuro mantenimiento por parte del personal el back end de la aplicación se escribirá la lógica de negocio en código java, mas adelante se detallaran mejor el uso de este lenguaje. Para publicar el sistema en la web se utilizara el servidor de aplicaciones tomcat de apache, donde se empaquetara en un archivos .war la aplicación ha ser desplegada por el servidor. La elaboración y pruebas del sistema se llevaran a cabo con el gestor de base de datos mysql.

En vista de las herramientas que se utilizaran para cumplir con los requerimientos antes establecidos se tendrá que utilizar servicios adicionales para la comunicación ha ser establecida entre el back end escrito en java y el front end que va a ser implementado en action script, por lo que en este punto se considero el uso de herramientas que proporcionen el servicio de datos como lo es "GraniteDS" para J2EE



Application Servers, que es una implementación de software libre u open source publicado bajo la licencia LGPL V2, es el equivalente a livecycle que es su similar de pago propiedad de Adobe, este servicio de datos establece un canal de comunicación mediante el protocolo de intercambio de datos AMF3 (introducido por adobe) entre el back end echo en java y el front end echo en javascript. Es decir GraniteDS provee un framework para aplicaciones que utilicen el motor de flash como flex3 y ayuda a la transmisión de los denominados objetos remotos entre el front y el back end a través de servicios de datos. A continuación se muestra un grafico que detalla el modelo de Granite DS.

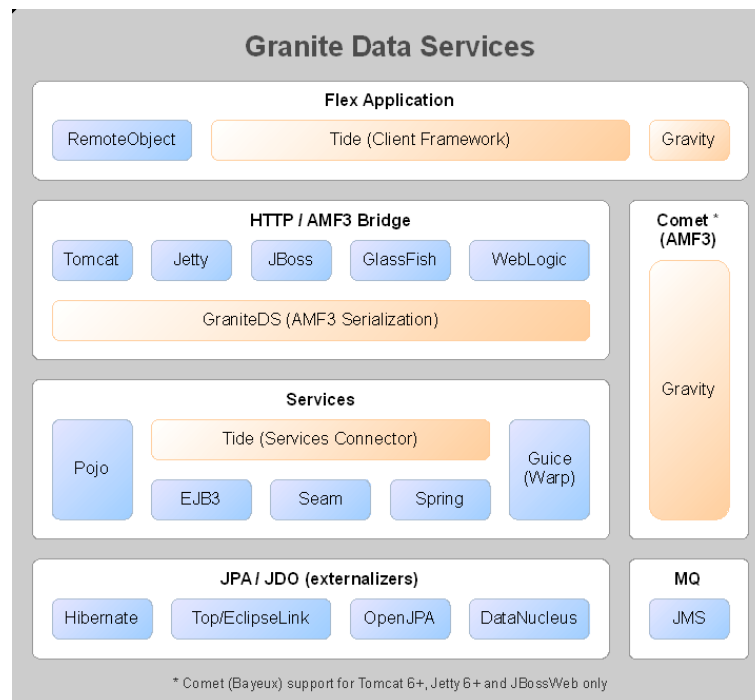


Figura 2.18 Granite Data Services⁴

A continuación se detallaran las herramientas a ser utilizadas en la construcción del sistema.

⁴ Imagen, Arquitectura Granite DS, fuente: <http://www.graniteds.org/confluence/pages/viewpage.action?pageId=22937>



Bases de datos.

MySQL será el gestor de base de datos que se utilizara en el desarrollo y pruebas del sistema dado su facilidad de uso y que utiliza el clásico modelo relacional utilizado también por DB2 que es el motor de base de datos utilizado en la institución para sus sistemas.. Siendo también una de las razones más importantes el hecho de que a pesar de que su desarrollo este a cargo de una empresa privada cuenta con una licencia GNU GPL:

MySQL presenta buenas características funcionales y la flexibilidad necesaria para el sistema, cuenta con soporte para varios lenguajes de programación que han desarrollado APIs nativas en el caso del lenguaje JAVA que nos interesa, este tipo de APIs se adaptan de una manera integra y proporcionan seguridad a la hora de realizar operaciones transaccionales en la base de datos.

Para la gestión mysql se cuenta con interfaces graficas así como de líneas de comando para todo tipo de plataformas, en nuestro caso vamos a utilizar un gestor web llamado Phpmyadmin muy conocido basado en php.

Lenguajes de Programación.

Java

Se menciona con anterioridad el requisito de que el modelo de negocio del sistema sea implementado en Java ya que este lenguaje de programación es uno de los mas conocidos y utilizados para el



desarrollo de aplicaciones, es orientado a objetos, y dado que es independiente de la plataforma el departamento de sistemas del Empresa eléctrica lo ha tomado como estándar para sus sistema.

Mediante el uso de la maquina virtual java que se ha desarrollado para cada sistema entre los que se incluyen los mas importantes como Linux en nuestro caso, dicha maquina virtual hace de puente entre la aplicación y el sistema operativo. Lo que permite un desarrollo bajo cualquier sistema operativo, lo que brinda la posibilidad directa de trabajar sobre una distribución open source como Linux Ubuntu durante el desarrollo.

Es importante indicar que el lenguaje java posee una licencia GNU GPL publicada e el año 1996 por la empresa que lo desarrollo, de tal manera que todo el Java Sun es ahora software libre. Java posee su propia tecnología para desarrollar en la plataforma web como son applet que son pequeñas aplicaciones que pueden incrustarse en el código HTML, esto del lado del cliente, y si consideramos el lado del servidor java también esta presente con servlet y JSP. De esta manera podemos decir que java posee un gran soporte para integrarse con herramientas que trabajan del lado del cliente, por lo que será utilizada del lado del servidor en el presente proyecto.

En vista de esta elección en cuanto al lenguaje de programación para el backend se ha seleccionado el IDE Eclipse como el idóneo para integrar todas las herramientas adicionales, ya que a mas de ser software libre, es muy flexible en la integración de nuevas componentes., para la



elaboración del presente proyecto de utilizara la versión: eclipse-jee-galileo-SR2-linux-gtk.

Action Script

Dada la necesidad presente de contar con una interfaz RIA para el sistema se eligió el uso del lenguaje Action Script en su versión 3.0 denominado también AS3 que es orientado a objetos, ya que este lenguaje emitido por la Empresa Adobe, esta orientado al desarrollo de aplicaciones Web animadas o conocidas como RIAs mas concretamente. Action Script es un lenguaje de script lo que indica que no requiere que un programa completo para realizar las acciones para las que fue escrito.

Como el lenguaje esta basado en el mismo estándar de Javascript facilita los procesos de mantenimiento del sistema por parte del personal de la empresa que si están familiarizados con la tecnología JavaScript. Adobe incluye Action Script 3 en su versión de Adobe Flash, así también el SDK de Flex que es de software libre y se encuentra en su versión 4 con soporte para la plataforma Linux el cual será utilizado y detallado mas adelante.

Ya que la aplicación se desarrollara en Action Script para la interfaz, esta se ejecutara como una aplicación en Flash player, por lo que los browser deben tener soporte del reproductor flash player, lo que no representa inconveniente ya que el reproductor de flash player es muy difundido y



tiene versiones para todos los navegadores en general así como para todas las plataformas.

La compatibilidad que presenta el lenguaje AS3 con tecnologías como google maps con la **“Referencia del API de Google Maps para ActionScript”** lo que permite cumplir una de las necesidades del proyecto de contar con una referencia geográfica de la ubicación de los elementos que maneja, las facilidades que brinda al usuario final en el manejo de la aplicación y el fácil desarrollo de la aplicación que representa para el programador siendo esta compatible con un backend basado en Java resulta la opción adecuada a tomar en cuenta

Frameworks de Programación

FLex será el framework base para el desarrollo de la interfaz de usuario ya que fue concebido para la creación de aplicaciones web y es un marco de trabajo de código abierto y gratuito, el lenguaje esta basado en etiquetas XML y ActionScript que esta considerado como el lenguaje del lado del cliente.

Montar un servidor de presentación Flex en la plataforma J2EE que tendrá el sistema no presenta problemas ya que se trata de una aplicación Java nativa. El despliegue de la aplicación Flex en la plataforma J2EE se maneja con archivos web Java de extensión WAR.

Arquitectura del Framework

Una de las ventajas en Flex al crear la interfaz de usuario es que se ejecuta en la máquina virtual y omnipresente de Flash Player. Mientras



se ejecuta en el Flash Player, la aplicación Flex puede interactuar con la funcionalidad del lado del servidor, mediante Data Services como granite DS, objetos remotos Java, servicios web SOAP y otros servicios del lado del Servidor para aplicaciones Java como Apache Tomcat servlet container que sera utilizado en el presente proyecto. A continuación se presenta un grafico del modelo utilizado por el Servidor de presentación Flex.

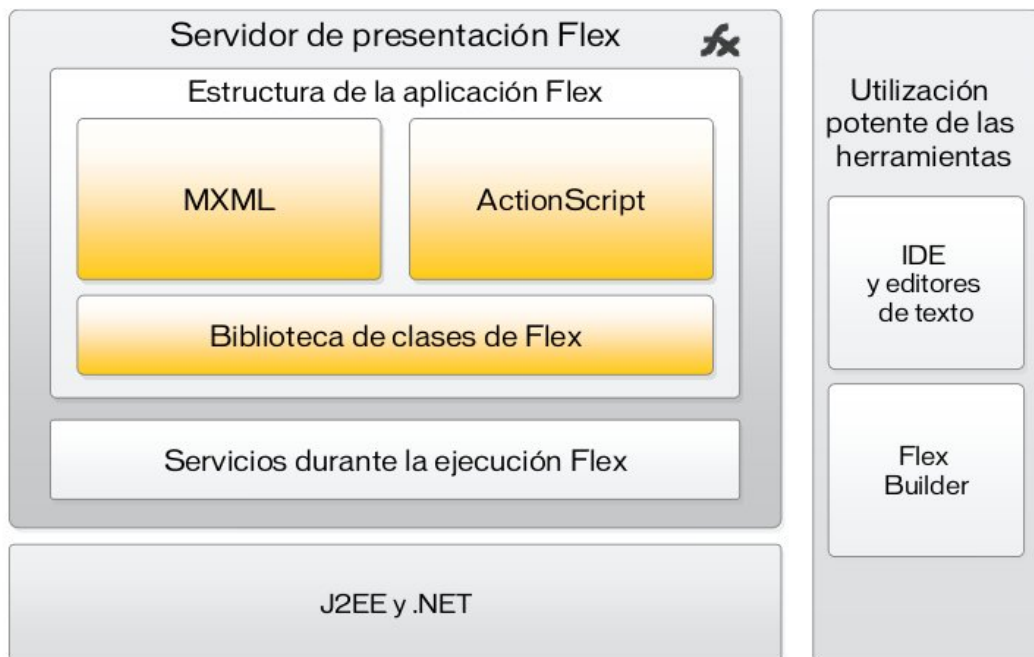


Figura 2.19 Servidor de presentación Flex

Como se ve en la grafica una aplicación Flex está compuesta por:

- El MXML que se usa para definir declarativamente los elementos de la interfaz del usuario



- ActionScript para la lógica del cliente y el control de los procedimientos.
- Una biblioteca de clases dinámicas que contiene componentes Flex (contenedores y controles), enlaces de datos, comportamientos y otras características

La biblioteca de clases de Flex proporciona dos tipos de componentes que serán utilizados en la aplicación:

Los **controles** son componentes de la interfaz de usuario que manejan las interacciones del mismo y muestran datos que los usuarios pueden manipular directamente a través de ese control.

Un **contenedor** define una región de la superficie de dibujo del Flash Player y controla la disposición para todo en el contenedor en lo que se refiere a la interfaz e Usuario.

Servidores y servicios en tiempo de ejecución.

Una aplicación Flex tiene un modelo de compilado que se denomina “justo a tiempo”. Flex es una herramienta que nos sirve para el desarrollo de aplicaciones web RIA y según este modelo una aplicación Flex se compila la primera vez que se acude a ella y se carga en su totalidad, y luego se mantiene en la memoria caché, y según se vayan realizando invocaciones subsiguientes se recompilan automáticamente si se actualiza cualquier archivo relacionado.



Para la integración de la herramienta se ha utilizado el plugin de Flex Builder para Linux que se integra un editor de ficheros MXML al IDE Eclipse, para el presente proyecto se utiliza la siguiente versión:

flexbuilder_linux_install_a5_112409.bin

API

WebNMS

Ya que la aplicación requiere el monitoreo a través de snmp se ha seleccionado una herramienta que proporciona la posibilidad de trabajar desde el entorno J2EE directamente equipos de la red centrosur IP/MPLS, esta herramientas es WebNMS, un API desarrollado en base a estándares del protocolo SNMP que cuenta con us propio framework en su version comercial. Este API desarrollada en java facilita la implementación de soluciones empresariales echas a la medida de las necesidades del sistema ya sean de tipo Element Management System (EMS) o Network Management System (NMS) que es el caso del presente sistema. Para el desarrollo de las aplicaciones de tipo NMS el framework WeNMS utiliza las funcionalidades del protocolo SNMP en sus diferentes versiones.

El API ofrece un completo kit de herramientas para el desarrollo de aplicaciones pensadas para el manejo de redes como el monitoreo en tiempo real y rastreo de elementos de red, este API esta compuesto por un conjunto de librerías Java SNMP.

Arquitectura del API



Universidad de Cuenca

El API posee un conglomerado jerárquico de paquetes java permitiendo de esta manera el desarrollo de aplicaciones en una gran variedad de plataformas y por supuesto la integración con el backend del sistema de tesis.

El API esta basado en diferentes niveles de acceso que permite el desarrollo a usuarios que tienen un conocimiento profundo de SNMP. Para el caso del sistema donde la implementación del uso de snmp se basa en monitoreo se trabajara a un nivel superior.

En el desarrollo del modulo de monitoreo se utilizara el API en un alto nivel, a continuación se presenta el grafico con la arquitectura del API desarrollado por WebNMS.



Grafico de Arquitectura del API

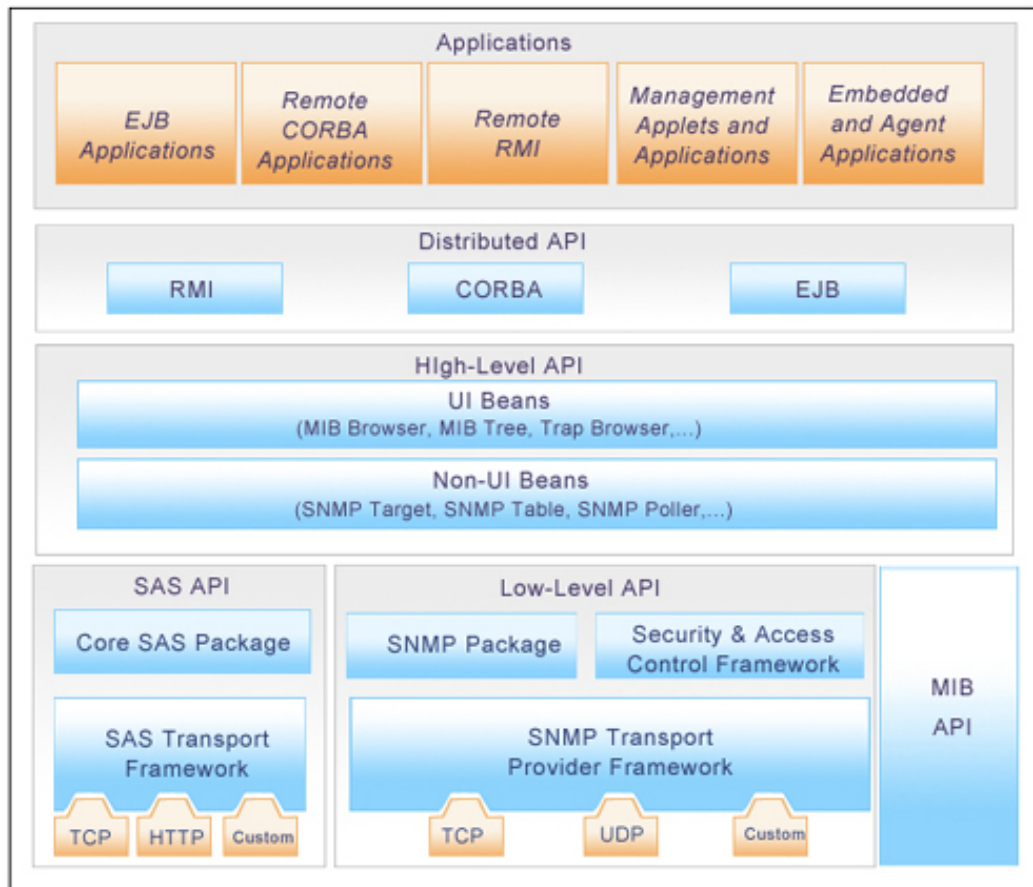


Figura 2.20 Grafico de arquitectura del API

High-Level SNMP API

El desarrollo del modulo se basa en el uso de un set de UI and non-UI java beans construidos a partir de las funciones de bajo nivel del API que se adaptara al IDE Eclipse de Java.

El propósito de usar High level API es facilitar el desarrollo usando los métodos de librerías SNMP para obtener la información de los agentes snmp. Mediante el uso de Java Beans evitando la complejidad del uso del API a bajo nivel.



La API implementa UDP/IP como el protocolo por defecto y provee TCP/IP como una implementación de referencia

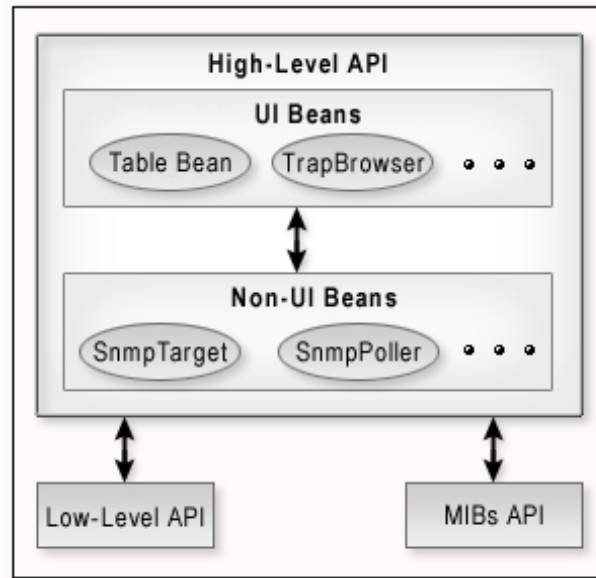


Figura 2.21 High-Level SNMP API⁵

Los siguientes son algunos de los componentes a ser tomados en cuenta del paquete beans en el desarrollo del modulo de monitoreo

Componentes no-UI, paquete beans

- *SnmpTarget* – se utiliza para sincronizar las operaciones SNMP que se van a realizar.
- *SnmpRequestServer* - se utiliza para realizar operaciones SNMP de manera asíncrona
- *SnmpPoller* – para realizar polling SNMP
- *SnmpTrapReceiver* – utilizado para la recepción de traps.

⁵ High Level Api, WebNMS fuente:
http://www.webnms.com/snmp/help/snmpapi/snmpv3/api_overview/highlevelapiarch.html



- NotificationAdaptor – este componente debe ser usado conjuntamente con TrapReceiver para la recepción de traps

Requerimientos del Sistema para el uso del API SNMP

Los siguientes son los requerimientos de hardware y software que el sistema debe poseer para trabajar con el API de webNMS:

Sistema Operativo	Windows, Solaris y Linux platforms.
Requerimientos de Hardware	CPU: minimo 500 MHz Pentium Processor Memory: minimo 128 MB RAM Disk Space: minimo 150 MB
Requerimientos de Software	JDK 1.2 y posteriores. Java-enabled web browser (Netscape 4.x/IE 4.x) con Sun Java plug-in. Cualquier database y el correspondiente JDBC driver

Servidor Web

Para la aplicación no se utilizara un servidor web como tal, ya que esta construida en java y compilada junto con el código de interfaz del lado del usuario escrito en action script, por lo que se tiene que ejecutar en un repositorio de aplicaciones que soporte servlet y applets, y la opción mas



adecuada para tal fin es Apache Tomcat, una implementación de Java que crea un contexto que sirve de contenedor de servlets. Para la aplicación de tesis Tomcat maneja Web-Archives que son empaquetados con extensión .war que contiene la estructura de archivos de una aplicación web, esta estructura es la siguiente:

Directorio raíz: aquí se publican los ficheros estáticos (HTML, imágenes, hojas de estilo, etc.) y JSPs, contiene los siguientes subdirectorios:

Directorio WEB-INF: contiene el web.xml. Este fichero configura la aplicación. Por ejemplo, permite declarar servlets, asignarles parámetros de inicio, declarar alias y filtros, etc. Es decir define los parámetros q son usados cuando la aplicación se despliega en el contener de servlet Tomcat. Los 2 parámetros fundamentales del fichero son:

- 1.- Listener - es la clase java q se llama cuando se inicia y se detiene la aplicación.
- 2.- welcome file list - punto de entrada de la aplicación.

Directorio META-INF: context.xml, este archivo define los detalles del contexto de la aplicación.

Directorio classes: debe contener los ficheros compilados (servlets, beans, etc.) de las clases utilizadas por la aplicación web.

Directorio lib: debe contener otras bibliotecas de clases adicionales (comprimidas con jar) que utilice tu aplicación.



Los demás subdirectorios: se utilizaran dentro del sistema para ficheros estáticos

Automatización de Procesos

Tool Command Language

Para la automatización de los procesos se ha seleccionado Expect que es una extensión de Tool Command Language o TCL es un lenguaje de script creado por John Ousterhout, como un lenguaje interpretado, y su código puede ser creado y modificado dinámicamente. Es un lenguaje multiplataforma, con intérpretes que se ejecutan sobre Windows, Linux, UNIX, MacOS y OSX. A continuación se describe la herramienta y el uso que se le dará dentro del sistema.

Expect

Expect es una herramienta para automatizar aplicaciones interactivas tales como telnet, ftp, passwd, fsck, rlogin, tip, etc. Fue escrito por Don Libes. Expect utiliza pseudo terminales para interactuar con los procesos de manera transparente.

Expect se puede ejecutar a intervalos regulares a través del uso de cron para encapsular tareas de administración del sistema. Esto se da gracias que expect utiliza las herramientas de administración que ya se encuentran en el sistema.

En la Industria es utilizado por una gran cantidad de empresas como Silicon Graphics, IBM, HP, Sun, Xerox, Amdahl, Tektronix, AT&T,



ComputerVision and the World Bank para automatizar, transferencia de archivos, administración de cuenta, y pruebas de networking, etc.

Expect posee módulos que han sido portados para el lenguaje Java, Python, Perl. En el caso del sistema se utilizara los módulos correspondientes al lenguaje Java.

El inconveniente que presenta es la portabilidad ya que si creamos un script expect que utiliza varias herramientas nativas Unix no podremos utilizarlo en un sistema como Windows. Dicha desventaja, será aprovechada por el sistema como una ventaja ya para las tareas de automatización se utilizaran las propias herramientas de configuración de los equipos de red.

ExpectJ

ExpectJ es una Implementación Java de la herramienta Unix Expect TCL, ExpectJ provee un soporte parecido al de Expect y permitirá escribir los programas en Java que se comunicaran con los equipos de red para la automatización en la configuración de los parámetros de red

Estructura del Paquete:

Todas las clases ExpectJ están localizadas en el paquete “expectj”, este paquete incluye 2 clases que manejan la interacción que brinda Expect

Clase: expectj.ExpectJ



ExpectJ es el punto de entrada de la API. ExpectJ actúa como un contenedor de procesos spawning y donde se realizan otras funciones de tipo ExpectJ

Constructor:

ExpectJ(String sLogFile, long IDefaultTimeOut)

Este constructor crea un objeto Expect. Este objeto puede ser usado para la comunicación y generación de diferentes procesos. Algunas definiciones a tomar en consideración para esta clase son:

sLogFile es la ubicación de archive de log donde ExpectJ escribe sus mensajes de debug.

IDefaultTimeOut.- es el valor por defecto del tiempo de espera para los comandos expect. Un valor de -1 por defecto indica un tiempo de espera indefinido.

Métodos:

spawn(StringsCommand)

Este método genera un proceso sCommand en un hilo de proceso diferente y retorna un objeto SpawnedProcess el cual se utiliza para comunicarse con el proceso generado por el comando spawn. Un objeto ExpectJ se puede usar para generar tantos procesos como sean necesarios, en cambio un objeto SpawnProcess representa solo un proceso.

Clase: expectj.SpawnedProcess



Esta clase representa un proceso generado y todas las comunicaciones con este proceso pueden hacerse usando el objeto que retorna ExpectJ.Spawn.

Métodos

`expect(String pattern, long ITimeOut) throws ExpectJException`

Este método funciona igual que el comando Expect de Unix. Este espera por leer el string respuesta del proceso generado.

ITimeOut es el tiempo de espera en segundos que el comando expect va a esperar por la respuesta del proceso, una timeout de -1 hará que el método expect espere indefinidamente por una respuesta del proceso

`expect(String pattern) throws JExpectException`

Este método funciona exactamente como se describió el proceso expect anteriormente, pero utiliza el tiempo de espera por defecto especificado en el constructor ExpectJ.

`expectErr(String pattern, long ITimeOut) throws JExpectException`

Este método funciona igual que la función expect excepto que trata de comparar el patrón con la salida de secuencia de error estándar del proceso generado en un tiempo de espera determinado.

`expectErr(String pattern) throws JExpectException`



Este método funciona igual que la función `expect` excepto que trata de comparar el patrón con la salida de secuencia de error estándar del proceso generado.

`isLastExpectTimeOut()`

Este método regresa `true` si el último método `expect()` o `expectErr()` retornó debido a que el tiempo de espera expiró en lugar de obtener una respuesta del proceso

`send(String line) throws JExpectException`

Este método envía el string como entrada del proceso generado, si el proceso ya ha terminado se lanza una `JExpectException`.

`isClosed()`

Este método retorna `true` si el proceso ya ha finalizado. Este método debería ser utilizado para revisar el estado del proceso antes de usar el método `send()`.

`getExitValue()`

Este método retorna la salida del código de el proceso si el proceso ya ha terminado

`stop()`

Este método mata el proceso representado por el objeto de tipo `SpawnedProcess`.



3.2 DISEÑO

3.2.1 Arquitectura del sistema

El sistema establecerá una conexión directa con la red de comunicación IP/MPLS a través de la interfaz de red del equipo Servidor hospedero donde estará instalada la aplicación prototipo. Los módulos se implementarán en el backend de manera que la carga del procesamiento se realice únicamente en el server y no en el cliente, el módulo de configuración interactuará conjuntamente con los demás módulos para realizar las tareas que contemplan tanto el uso de información de clientes, usuarios y direccionamiento de manera íntegra en la gestión de configuración de los equipos de red. El sistema automatizará la configuración de los enlaces (capa 3 del modelo OSI) activos en la red IP/MPLS.

Diagrama de bloques

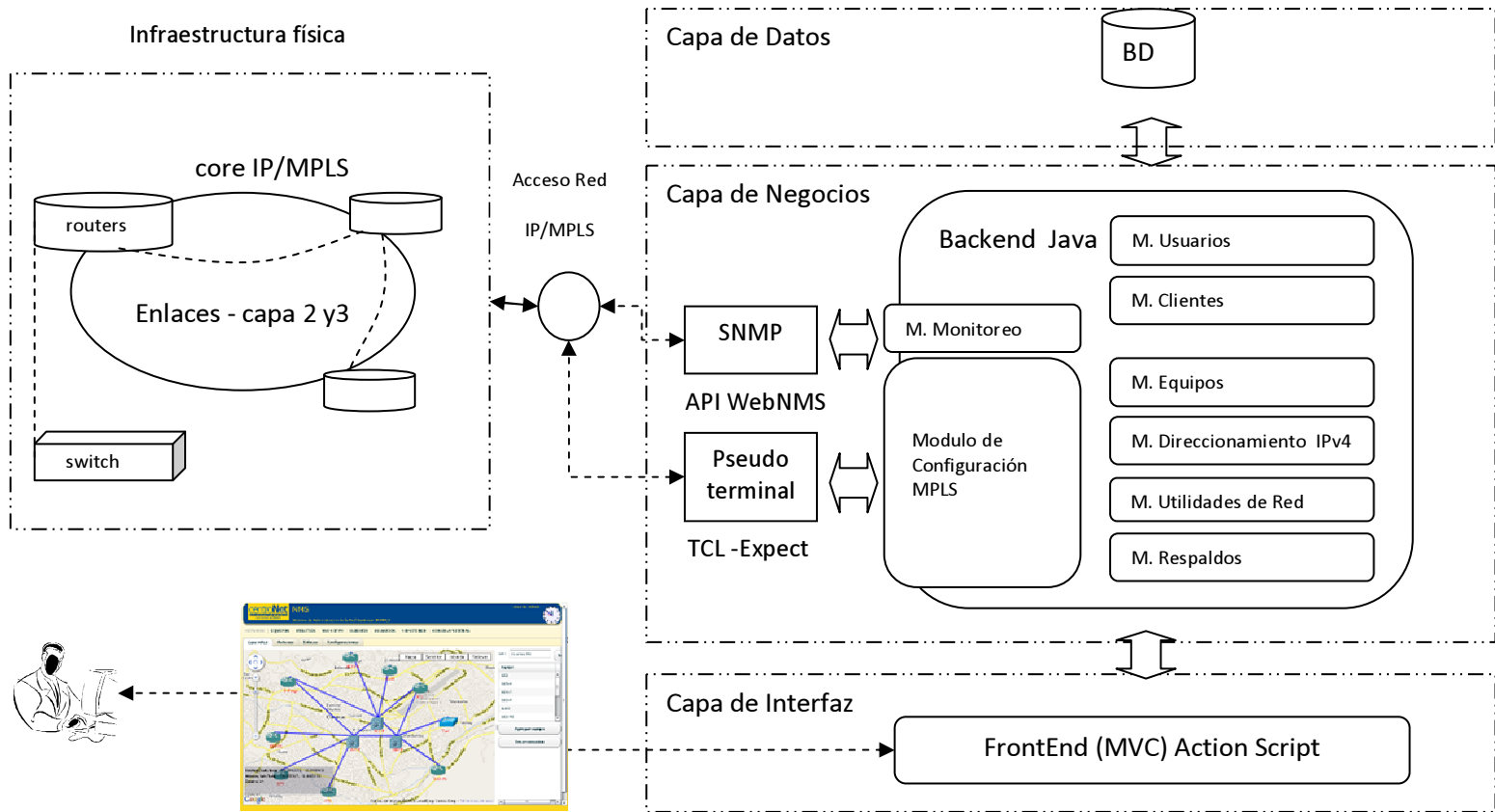


Figura 2.22 Diagrama de bloques

Modelo Cliente Servidor

Dado que el sistema esta pensado como una Aplicacion RIA (Rich Internet Applications) que es la unión entre las ventajas que presentan las aplicaciones tradicionales de escritorio y las aplicaciones web donde se eliminan las deficiencias de las aplicaciones web tradicionales donde al refrescar un cambio se tiene que actualizar toda la página, mientras que en un entorno web RIA desde el inicio se carga toda la aplicación y solo se produce comunicación con el servidor cuando se requieran datos de la Base de Datos.

La arquitectura de aplicaciones web RIA se basa en el modelo cliente-servidor, en donde el cliente se encarga de la interacción entre la interfaz y el usuario. El cliente es el encargado de mantener el estado de la aplicación ya que se controlan las vistas y la forma de cómo se muestran los datos.

Mientras que el Servidor es el encargado de gestionar las peticiones del cliente, que son directamente operaciones en la base de datos.

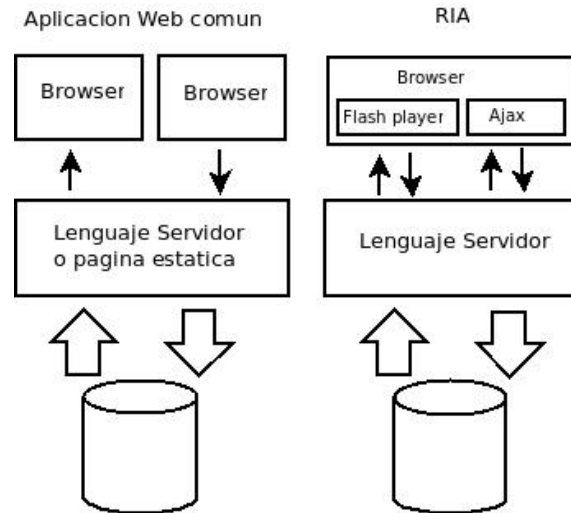


Figura 2.23 **Modelo Cliente Servidor**

Aquí observamos el modelo (derecha) de la aplicación utilizada en el sistema de tesis que se ejecuta en 2 entidades, el browser donde se ejecuta Flash Player y Ajax representa la parte cliente y mas abajo en otro nivel el lenguaje del servidor, comparado con una aplicación web tradicional (izquierda) realiza todo el procesamiento de datos en el servidor, y usa el Navegador o Browser solo para mostrar la información resultante del procedimiento, y teniendo que volver a cargar todo el contenido de la pagina cuando hay algún cambio.

Arquitectura de programación MVC

Para mantener una adecuada programación de la interfaz se ha elegido la arquitectura MVC o Modelo Vista Controlador que es un patrón de diseño de programación que se fundamenta en segmentar el código en componentes bien definidos de la futura aplicación, siendo estos:



- Modelo.- es una representación de la lógica de negocio y el manejo del sistema de base de datos MySQL
- Vista.- es la interfaz que tiene una actualización dinámica de las vistas del sistema, incluyendo mapas de localización, grillas etc.
- Controlador.- Sera el encargado de gestionar los eventos q son acciones del usuario como recibir datos desde la vista, e interactúa entre el modelo de donde toma datos y enviándolos a la vista

El siguiente grafico representa la arquitectura MVC aplicada a un entorno de programación que gestiona el patrón de programación MVC del lado del cliente donde se incluirá un entorno JAVA J2EE del lado del servidor.

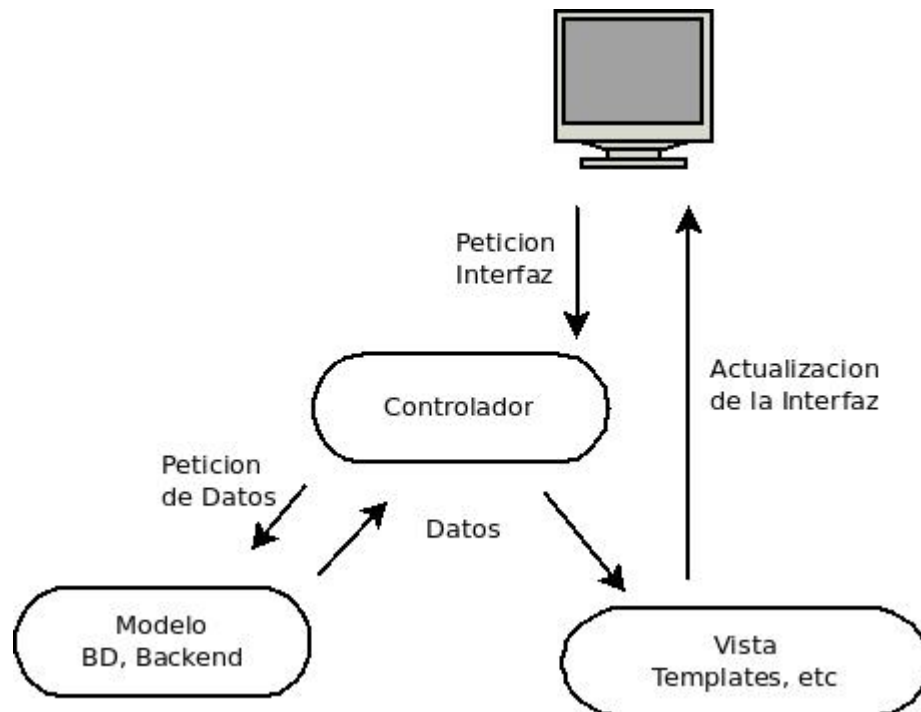


Figura 2.24 Arquitectura de programación MVC



En este ejemplo vemos que una petición de un usuario es recibida directamente por el controlador mediante un evento generado en la interfaz de usuario, el controlador es el encargado de gestionar las transacciones dirigidas a la base de datos y que serán procesadas por el servidor a través de servicios web, dependiendo de los resultados de las transacciones que son devueltos al mismo controlador que actualiza el modelo que a su vez abastece y actualiza a la vista.

3.2.2 Actores

- Administrador del sistema.-Esta persona estará a cargo de la creación de usuarios y la asignación de roles y configuración de módulos y sub módulos
- Administrador de red.- Persona que llevara un control/monitoreo total de las tareas de configuración realizadas en el sistema, administración de equipos, enlaces, VRFs, direccionamiento IP o tareas de respaldos.
- Asistente.- persona que realizará las tareas de administración más básicas en el sistema como monitoreo, ingreso de vrf.
- Soporte.- persona que tendrá las mismas facultades del asistente y aparte cumple tareas de soporte directamente con los clientes de la Empresa, por lo que su rol dentro del sistema lo consideramos del mismo tipo del asistente.



Figura 2.25 Actores

3.2.3 Casos de Uso

A continuación se listan los casos de uso del sistema, los cuales serán descritos con más detalle mas adelante.

- 0 Login de usuario
- 1 Ingreso de Usuario
- 2 Eliminación de Usuario
- 3 Actualización Usuario
- 4 Búsqueda Usuario
- 5 Reportes de Usuarios
- 6 Ingreso de VRF
- 7 Eliminación de VRF
- 8 Actualización VRF
- 9 Búsqueda de VRF
- 10 Ingreso de un equipo
- 11 Eliminación de un equipo
- 12 Actualización de un equipo
- 13 Búsqueda de un equipo



14 Respaldo Información de la configuración de un Equipo

15 Cargar un respaldo de un equipo

16 Reporte del estado de un equipo

17 Calculo de Subredes

18 Ingresar subred

19 Eliminar una subred

Casos de Uso Internos:

- Ingresar Interfaz al equipo
- Ingresar tipo de Usuario
- Ingresar tipo de interfaz

Estos casos de uso son complementarios a los casos de uso que están nombrados con anterioridad.

Asignación de caso de uso por actor

Actor: Administrador de sistema

Usuarios

- Ingreso de un usuario.
- Modificar Usuario.
- Buscar Usuario.
- Eliminación de un usuario.
- Reporte de Usuarios.

Diagrama:

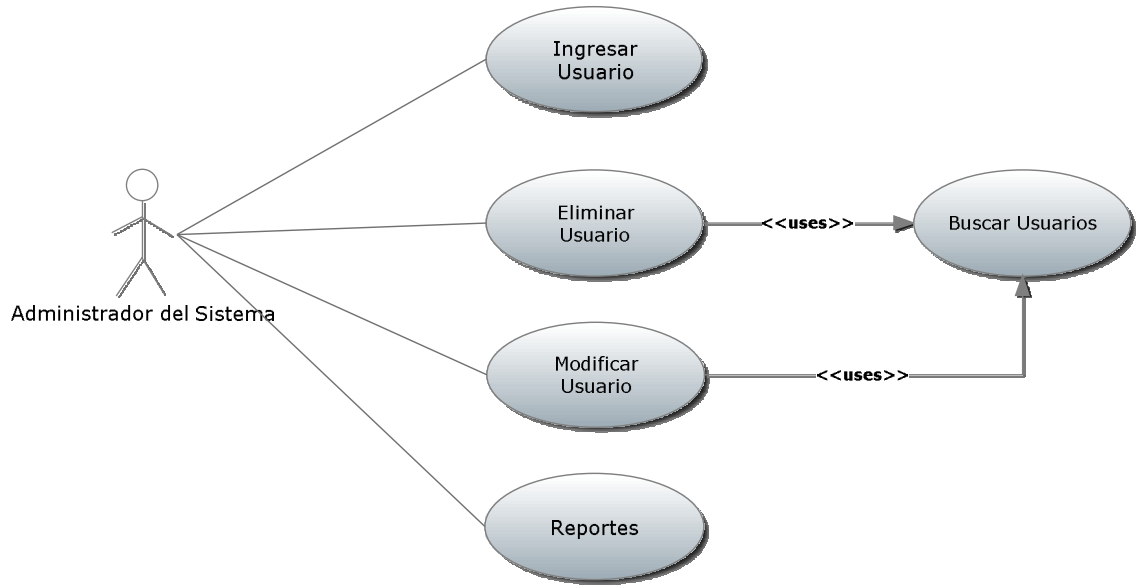


Figura 2.26 Administrador del sistema

Actor: Administrador de la Red

VRF

- Ingresar una VRF
- Eliminar una VRF
- Actualizar una VRF
- Buscar VRF

Equipos

- Ingreso de un equipo
- Eliminación de un equipo
- Actualizar un equipo
- Búsqueda de equipos
- Monitoreo estado de un equipo

Direccionamiento IP



- Calculo Subredes
- Ingresar una Subred
- Eliminación de Subredes

Respaldos de las configuraciones de los equipos

- Respaldar Información de la configuración de un Equipo

Diagrama:

DIAGRAMA DE CASOS DE USO: ADMINISTRADOR DE RED

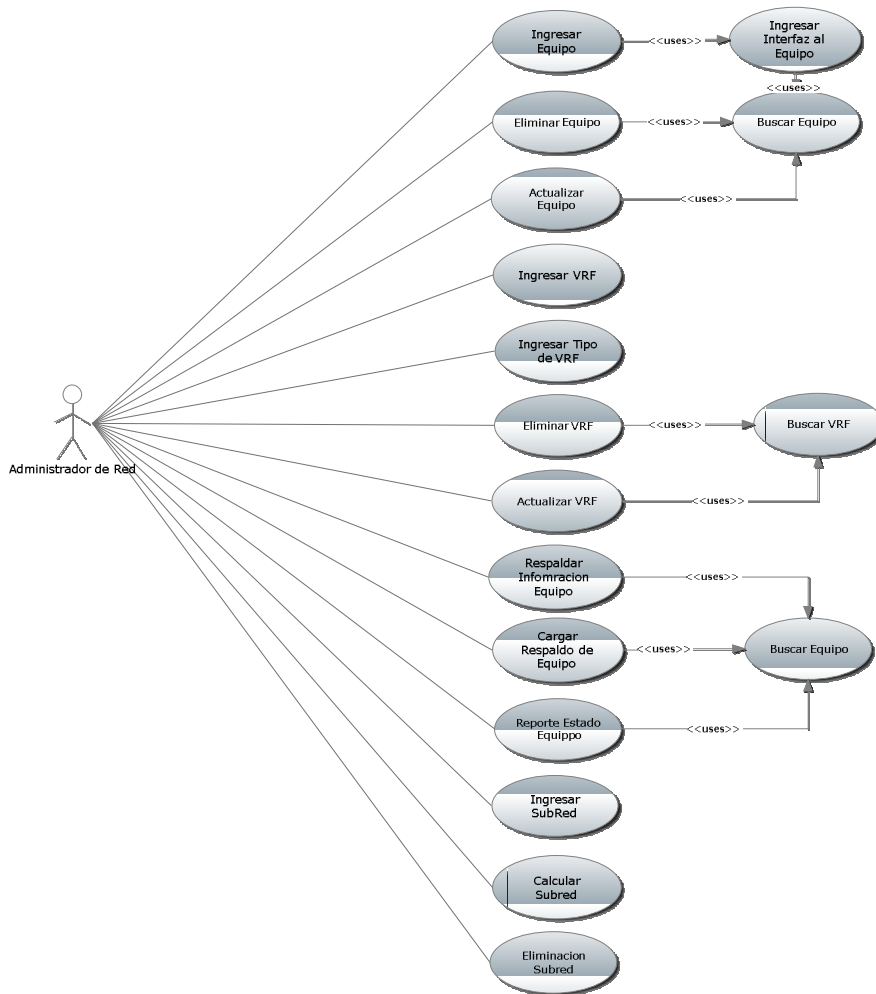


Figura 2.27 Administrador de la red



Actor: Asistente

VRF

- Ingresar VRFs
- Búsqueda de VRF

Equipos

- Ingreso de un equipo
- Búsqueda de equipos
- Informe del estado de un equipo

Direccionamiento IP

- Ingresar una Subred
- Calcular Subred

Respaldos de las configuraciones de los equipos

- Respaldar Información de la configuración de un Equipo
- Cargar un respaldo de un equipo

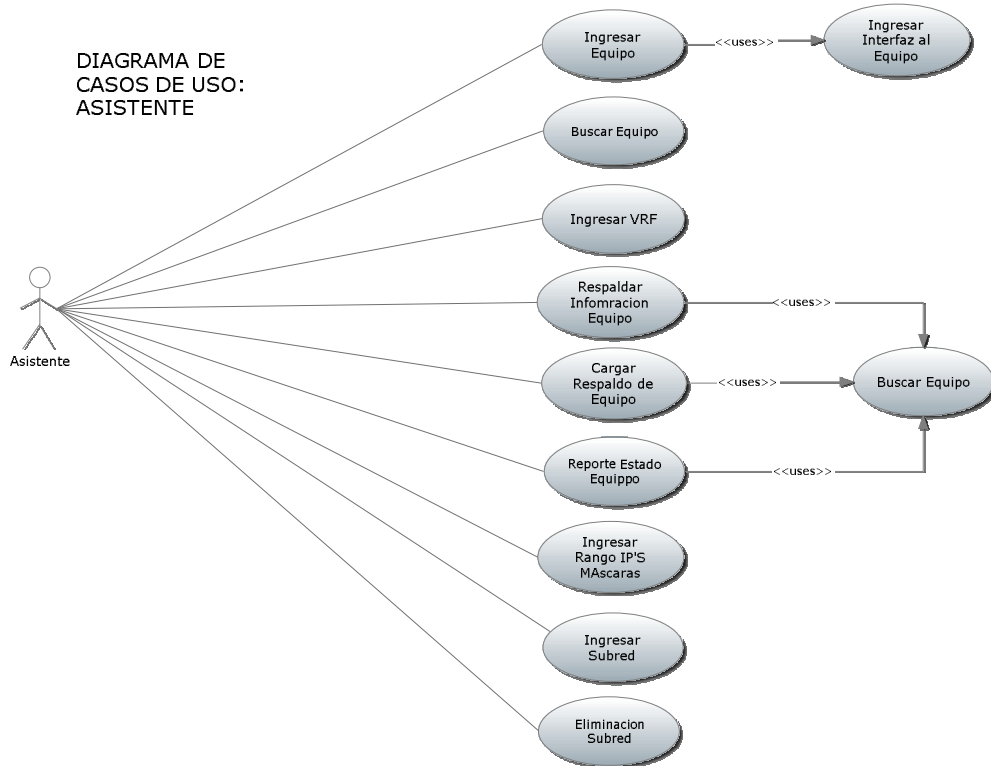


Figura 2.28 Asistente

A continuación se describen las fichas de los casos de uso del sistema que van a ser implementados:

Caso de Uso: 0	Login de Usuario
Descripción	La funcionalidad de este caso es el logeo validado de un usuario al sistema el cual tiene un rol ya ingresado anteriormente, el actor que interviene es el administrador del sistema, el administrador de la red y el asistente este caso de uso se realiza cuando el usuario quiere ingresar al sistema para las diversas tareas.
Flujo Básico	Inicio Despliega ventana con datos por ingresar El Usuario ingresa el nickname y el password Validación de los datos por el sistema. Se acepta el ingreso por el sistema Caso contrario despliega error Fin
Flujos Alternativos	Se realiza una búsqueda interna por el sistema del usuario con su nickname y password.



Precondiciones	No existe ninguna
Pos condiciones	No existe ninguna
Puntos de Extensión	No existe ninguna

Caso de Uso: 1	Ingresar Usuario
Descripción	La funcionalidad de este caso es el ingreso validado de un usuario para lo cual ya se tiene un rol ingresado anteriormente, el actor que interviene es el administrador del sistema, este caso de uso se realiza cuando se añade personal que va a interactuar con el sistema para los diversos roles.
Flujo Básico	Inicio Opción Ingresar Usuario Se ingresan los datos personales del usuario Validación de los datos. Se elige el rol del usuario de una combo o lista de roles de usuario. Se acepta el ingreso Fin
Flujos Alternativos	Activación de un Usuario Un usuario tiene dos estados: activo, no activo Si se produce que el administrador del sistema quiere ingresar un usuario anteriormente eliminado, el sistema solo pasa del estado no activo a un estado activo.
Precondiciones	El administrador del sistema debe logearse en el sistema por seguridad.
Pos condiciones	Para salir; el usuario escoge cancelar o salir de la ventana.
Puntos de Extensión	No existe ninguna

Caso de Uso: 2	Eliminar Usuario
Descripción	La funcionalidad de este caso es la eliminación lógica de un usuario, no es una eliminación física, el actor que interviene es el administrador del sistema este caso de uso se realiza cuando se da de baja a personal.
Flujo Básico	Inicio Logearse administrador del sistema



	<p>Opción eliminar Usuario Se realiza un caso de uso interno del sistema que es la búsqueda. Se acepta la eliminación. Fin</p>
Flujos Alternativos	<p>El usuario eliminado pasa de estado activo a estado no activo. No se visualiza en la lista de usuarios activos.</p>
Precondiciones	<p>El administrador del sistema debe logearse en el sistema por seguridad. El usuario debe existir y estar en modo activo. Se realiza una búsqueda de los usuarios activos.</p>
Pos condiciones	<p>Tiene la opción de seguir eliminando, para salir del mismo. Regresa al menú principal</p>
Puntos de Extensión	<p>No tiene operaciones o privilegios del usuario no activo. El usuario está en un estado no activo, y no podrá ingresar al sistema.</p>

Caso de Uso: 3	Actualizar Usuario
Descripción	<p>La funcionalidad de este caso es la actualización validada de un usuario, el actor que interviene es el administrador del sistema este caso de uso se realiza cuando se añade información personal o actualizaciones del usuario.</p>
Flujo Básico	<p>Inicio Logearse administrador del sistema Opción Actualizar Usuario Se realiza un caso de uso interno del sistema que es la búsqueda. Se modifican los campos que quiere Actualizar Se acepta la actualización Fin</p>
Flujos Alternativos	<p>Si el tipo de usuario fue modificado también sus operaciones según el rol del usuario actualizado</p>
Precondiciones	<p>El administrador del sistema debe logearse en el sistema por seguridad. El usuario debe existir y estar en modo activo. Se realiza una búsqueda de los usuarios activos.</p>
Pos condiciones	<p>Para salir; el usuario escoge cancelar o salir de la ventana.</p>



Puntos de Extensión	Los cambios en la información del usuario son actualizados en tiempo real. Las operaciones o privilegios son de acuerdo al tipo de usuario que obtiene.
---------------------	--

Caso de Uso: 4	Buscar Usuario
Descripción	La funcionalidad de este caso es la búsqueda de los usuarios, los actores que intervienen es el administrador del sistema, este caso de uso se realiza cuando se quiere eliminar o Actualizar un usuario específico.
Flujo Básico	Inicio Logearse administrador del sistema Opción Usuario Se muestra en una grilla todos los usuarios. El administrador del sistema escoge el usuario para la operación que selecciono. Fin
Flujos Alternativos	El administrador del sistema está un caso de uso que puede ser eliminación y actualización de un usuario.
Precondiciones	El administrador del sistema debe logearse en el sistema por seguridad. El administrador del sistema debe hacer una eliminación o actualización para que el caso de uso se realice.
Pos condiciones	Para salir; el usuario escoge cancelar o salir de la ventana.
Puntos de Extensión	No existe ninguna.

Caso de Uso: 5	Reportes de Usuarios
Descripción	La funcionalidad de este caso es generar reportes de las tareas de los diferentes usuarios que interactúan con el sistema tal información debe poder visualizarse periódicamente o por usuario específico, los actores que intervienen es el administrador del sistema, este caso de uso se realiza para consultoría de las actividades de los usuarios del sistema.
Flujo Básico	Inicio Logearse administrador del sistema



	<p>Opción Reportes Se ingresan dos fechas que indiquen el periodo que genera un reporte de los usuarios y sus actividades. Caso contrario se escoge la opción por usuario, Se ingresa el parámetro de búsqueda para buscar el usuario. Despliega una lista de todas las actividades que ha hecho el usuario. Fin</p>
Flujos Alternativos	<p>El sistema realiza una búsqueda por fecha o por el parámetro ingresado y genera reportes. El sistema realiza una búsqueda de actividades por usuario.</p>
Precondiciones	<p>El administrador del sistema debe logearse en el sistema por seguridad.</p>
Pos condiciones	<p>Para salir; el usuario escoge cancelar o salir de la ventana.</p>
Puntos de Extensión	<p>No existe ninguna.</p>

Caso de Uso: 6	Ingresar VRF
Descripción	<p>La funcionalidad de este caso es el ingreso validado de un VRF el cual tiene un tipo o categoría ya ingresado anteriormente, el actor que interviene es el administrador de la red y el asistente, este caso de uso se realiza cuando se añade VRFs nuevos al sistema.</p>
Flujo Básico	<p>Inicio Opción Ingresar VRF. Se ingresan los datos del VRF Validación de los datos. Se elige el tipo de VRF de un combo o lista de tipos de VRFs Se acepta el ingreso Fin</p>
Flujos Alternativos	<p>Activación de un VRF Un VRF tiene dos estados: activo, no activo Si se produce que el administrador de la red quiere ingresar un VRF anteriormente eliminado, el sistema solo pasa del estado no activo a un estado activo.</p>
Precondiciones	<p>El administrador del sistema debe Logearse en el</p>



	sistema por seguridad.
Pos condiciones	Para salir; el usuario escoge cancelar o salir de la ventana.
Puntos de Extensión	No existe ninguna.

Caso de Uso: 7	Eliminar VRF
Descripción	La funcionalidad de este caso es la eliminación lógica de un VRF, no es una eliminación física, el actor que interviene es el administrador de la red este caso de uso se realiza cuando se da de baja a un VRF.
Flujo Básico	Inicio Logearse administrador de la red Opción eliminar VRF Se selección la VRF de una grilla y se la manda a eliminar Se realiza un caso de uso interno del sistema que es la búsqueda. Se acepta la eliminación. Fin
Flujos Alternativos	El VRF eliminado pasa de estado activo a estado no activo. No se visualiza en la lista de VRFs activos.
Precondiciones	El administrador de la red debe Logearse en el sistema por seguridad. El VRF debe existir y estar en modo activo. Se realiza una búsqueda de los VRFs activos.
Pos condiciones	Para salir; el usuario escoge cancelar o salir de la ventana.
Puntos de Extensión	No tiene operaciones o privilegios del VRF no activo. El VRF está en un estado no activo, y no podrá ingresar al sistema.

Caso de Uso: 8	Actualizar VRF
Descripción	La funcionalidad de este caso es la actualización, el actor que interviene es el administrador de la red este caso de uso se realiza cuando se añade



	información personal o actualizaciones del VRF.
Flujo Básico	Inicio Logearse administrador del sistema Opción Actualizar VRF Se realiza un caso de uso interno del sistema que es la búsqueda. Se modifican los campos que se quiere Actualizar Se acepta la actualización Fin
Flujos Alternativos	Ninguno.
Precondiciones	El administrador del sistema debe logearse en el sistema por seguridad. El VRF debe existir y estar en modo activo. Se realiza una búsqueda de los VRFs activos.
Pos condiciones	Para salir; el usuario escoge cancelar o salir de la ventana.
Puntos de Extensión	Los cambios en la información del VRF es actualizada en tiempo real. Las operaciones o privilegios son de acuerdo al tipo de VRF que obtiene.

Caso de Uso: 9	Buscar VRF
Descripción	La funcionalidad de este caso es la búsqueda de los VRFs, los actores que intervienen es el administrador de red y su asistente, este caso de uso se realiza cuando se quiere eliminar o actualizar un VRF específico.
Flujo Básico	Inicio Logearse administrador de la red o el asistente Opción eliminar o Actualizar VRF Se realiza la búsqueda del VRF. Se muestra en una grilla todos los VRF. Opción ingresar VRFs de un VRF se realiza una búsqueda. El administrador del sistema escoge el VRF para la operación que selecciono. Fin
Flujos Alternativos	El administrador de la red está un caso de uso que puede ser eliminación y actualización de un VRF.



	El asistente está en un caso de uso ingreso de un VRF.
Precondiciones	El administrador de la red o el asistente debe Logearse en el sistema por seguridad. El administrador de la red debe hacer una eliminación o actualización para que el caso de uso se realice. El asistente debe hacer un ingreso de un VRF.
Pos condiciones	Para salir; el usuario escoge cancelar o salir de la ventana.
Puntos de Extensión	No existe ninguno.

Caso de Uso: 10	Ingresar Equipo
Descripción	La funcionalidad de este caso es el ingreso validado de un equipo, el actor que interviene es el administrador de la red y el asistente, este caso de uso se realiza cuando se añade Equipos nuevos al sistema.
Flujo Básico	Inicio Opción Ingresar Equipo. Se ingresan los datos del Equipo Validación de los datos. Se acepta el ingreso Fin
Flujos Alternativos	Ingreso Interfaz del equipo Es un caso de uso que puede ser ejecutado al ingreso del equipo, el actor decide si ingresa las interfaces o al Actualizar el equipo las realiza.
Precondiciones	El administrador de la red o el asistente debe logearse en el sistema por seguridad.
Pos condiciones	Para salir; el usuario escoge cancelar o salir de la ventana.
Puntos de Extensión	No existe ninguna.

Caso de Uso: 11	Eliminar Equipo
Descripción	La funcionalidad de este caso es la eliminación de un equipo, el actor que interviene es el administrador de la red y el asistente, este caso de uso se realiza



	cuando el equipo ya no está en uso.
Flujo Básico	Inicio Eliminar el equipo q se escoge de una grilla de equipos. Se acepta la eliminación. Fin
Flujos Alternativos	Ninguno.
Precondiciones	El administrador de la red o el asistente debe logearse en el sistema por seguridad. El equipo no debe tener vrf o conexión físicas relacionadas
Pos condiciones	La eliminación es lógica, pasa de un estado activo a un estado no activo. Para salir; el usuario escoge cancelar o salir de la ventana.
Puntos de Extensión	No existe ninguna.

Caso de Uso: 12	Actualizar Equipo
Descripción	La funcionalidad de este caso es la actualización validada de un Equipo, el actor que interviene es el administrador de la red y el asistente, este caso de uso se realiza cuando se añade información o actualizaciones del Equipo.
Flujo Básico	Inicio Logearse administrador del sistema Opción Equipo Se selecciona el equipo a Actualizar de la grilla en donde se encuentran listados todos los equipos Se modifican los campos que quiere Actualizar Se realiza un caso de uso interno del sistema que es la búsqueda. Clic en el botón para actualización Fin
Flujos Alternativos	Al realizar este caso de uso, puede usar el caso de uso Ingresar interfaz al equipo
Precondiciones	El administrador de la red o el asistente debe logearse en el sistema por seguridad. El Equipo debe existir y estar en modo activo. Se realiza una búsqueda de los Equipos activos.
Pos condiciones	Para salir; el usuario escoge cancelar o salir de la



	ventana.
Puntos de Extensión	Los cambios en la información del Equipos son actualizados en tiempo real.

Caso de Uso: 13	Buscar Equipo
Descripción	La funcionalidad de este caso es la búsqueda de los Equipos, los actores que intervienen es el administrador de red y su asistente, este caso de uso se realiza cuando se quiere eliminar o actualizar.
Flujo Básico	Inicio Logearse administrador del sistema Opción Equipo Se selecciona el equipo a Actualizar de la grilla en donde se encuentran listados todos los equipos Se modifican los campos que quiere Actualizar Se realiza un caso de uso interno del sistema que es la búsqueda. Clic en el botón para actualización Fin
Flujos Alternativos	El administrador de la red está un caso de uso que puede ser eliminación y actualización de un Equipo. El asistente está en un caso de uso ingreso de un VRF.
Precondiciones	El administrador de la red o el asistente deben ingresar en el sistema por seguridad. El administrador de la red debe hacer una eliminación o actualización para que el caso de uso se realice. El asistente debe hacer un ingreso de un VRF.
Pos condiciones	Para salir; el usuario escoge cancelar o salir de la ventana.
Puntos de Extensión	El equipo está en un estado no activo, y no podrá ingresar al sistema.

Caso de Uso: 14	Respaldar Información de la configuración de un Equipo
Descripción	La funcionalidad de este caso es hacer una copia de la información del equipo, los actores que intervienen son el administrador de red y su asistente, este caso de uso se realiza cuando se quiere obtener la



	información de configuración de los equipos y guardarla en un archivo.
Flujo Básico	Inicio Logearse administrador de la red o el asistente Opción Respaldar Información del Equipo. Se realiza la búsqueda del equipo. Se muestra en una grilla todos los Equipos y se selecciona el equipo. Opción respaldar Equipo. Aceptar Fin
Flujos Alternativos	Búsqueda de Equipos.
Precondiciones	El administrador de la red o el asistente debe logearse en el sistema por seguridad.
Pos condiciones	Para salir; el usuario escoge cancelar o salir de la ventana.
Puntos de Extensión	No existe ninguna.

Caso de Uso: 15	Cargar Respaldo de un Equipo
Descripción	La funcionalidad de este caso es cargar una copia de la información del equipo, los actores que intervienen es el administrador de red y su asistente, este caso de uso se realiza cuando se quiere obtener la información de un equipo y cargarla desde un archivo específico por el administrador.
Flujo Básico	Inicio Logearse administrador de la red o el asistente Opción Cargar Información del Equipo. Se realiza la búsqueda del equipo. Se muestra en una grilla todos los Equipos y se selecciona el equipo. Opción cargar información Equipo. Aceptar Fin
Flujos Alternativos	Búsqueda de Equipos.
Precondiciones	El administrador de la red o el asistente debe logearse en el sistema por seguridad.
Pos condiciones	Para salir; el usuario escoge cancelar o salir de la ventana.



Puntos de Extensión	No existe ninguna.
---------------------	--------------------

Caso de Uso: 16	Reporte Estado del Equipo
Descripción	La funcionalidad de este caso de uso es realizar un reporte de la información del equipo, los actores que intervienen son el administrador de red y su asistente, este caso de uso se realiza cuando se quiere obtener la información de un equipo: enlaces, VRF, interfaces, y monitoreo.
Flujo Básico	Inicio Ingresar como administrador de la red o como asistente. En el mapa que despliega al inicio se puede observar un gráfico con los equipos en donde se tiene que dar doble clic sobre los equipos para que desplieguen la información. Fin
Flujos Alternativos	ninguno
Precondiciones	El administrador de la red o el asistente debe logearse en el sistema por seguridad.
Pos condiciones	Para salir; el usuario escoge cancelar o salir de la ventana.
Puntos de Extensión	No existe ninguna.

Caso de Uso: 17	Calcular Subredes
Descripción	La funcionalidad de este caso es realizar un cálculo de una Subred para un grupo de equipos de la red, el actor que interviene es el administrador de la red y el asistente
Flujo Básico	Inicio Opción Ingresar Subred de IP's Opción calcular Subred. Acepta Fin
Flujos Alternativos	Se está realizando un ingreso de un nuevo Subred



	de IP's.
Precondiciones	El administrador de la red o el asistente deben logearse en el sistema por seguridad. Para entrar a este caso se debe primero ingresar al caso de uso Ingresar Subred de IP's
Pos condiciones	Para salir; el usuario escoge cancelar o salir de la ventana.
Puntos de Extensión	No existe ninguna.

Caso de Uso: 18	Ingresar Subred
Descripción	La funcionalidad de este caso es el ingreso validado de una Subred, los actores que interviene son el administrador de la red y el asistente, este caso de uso se realiza cuando se quiere Ingresar nuevas subredes al sistema.
Flujo Básico	Inicio Opción Ingresar Subred. Se ingresan los datos de la Subred Validación de los datos. Se acepta el ingreso Fin
Flujos Alternativos	Se puede realizar el caso de usos cálculo de Subredes.
Precondiciones	El administrador de la red o el asistente debe logearse en el sistema por seguridad.
Pos condiciones	Para salir; el usuario escoge cancelar o salir de la ventana.
Puntos de Extensión	Este Subred de IP's no se encuentra establecido, no se puede usar.

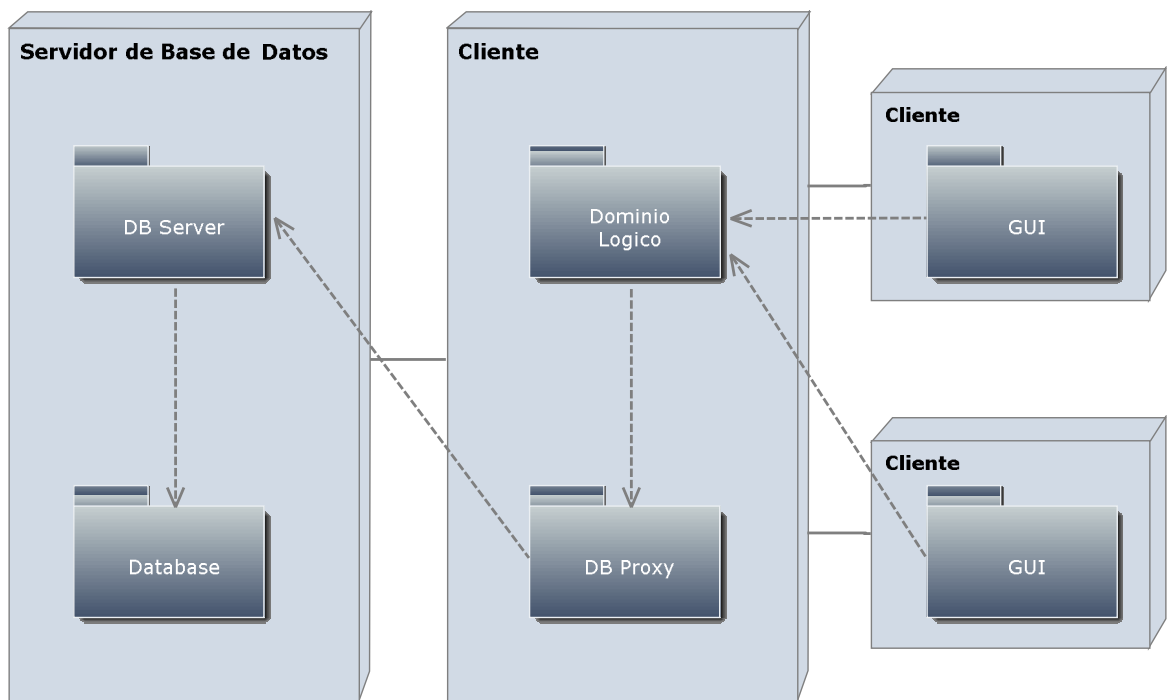
Caso de Uso: 19	Eliminar Subred
Descripción	La funcionalidad de este caso es eliminar una Subred, los actores que intervienen son el administrador de la red y el asistente.
Flujo Básico	Inicio Búsqueda de Subred establecidos en la grilla del sistema



	Selección de la subred a eliminar Opción eliminar Subred. Acepta Fin
Flujos Alternativos	Se puede realizar el caso de usos cálculo de Subredes.
Precondiciones	El administrador de la red o el asistente debe logearse en el sistema por seguridad.
Pos condiciones	Para salir; el usuario escoge cancelar o salir de la ventana.
Puntos de Extensión	No existe ninguna.

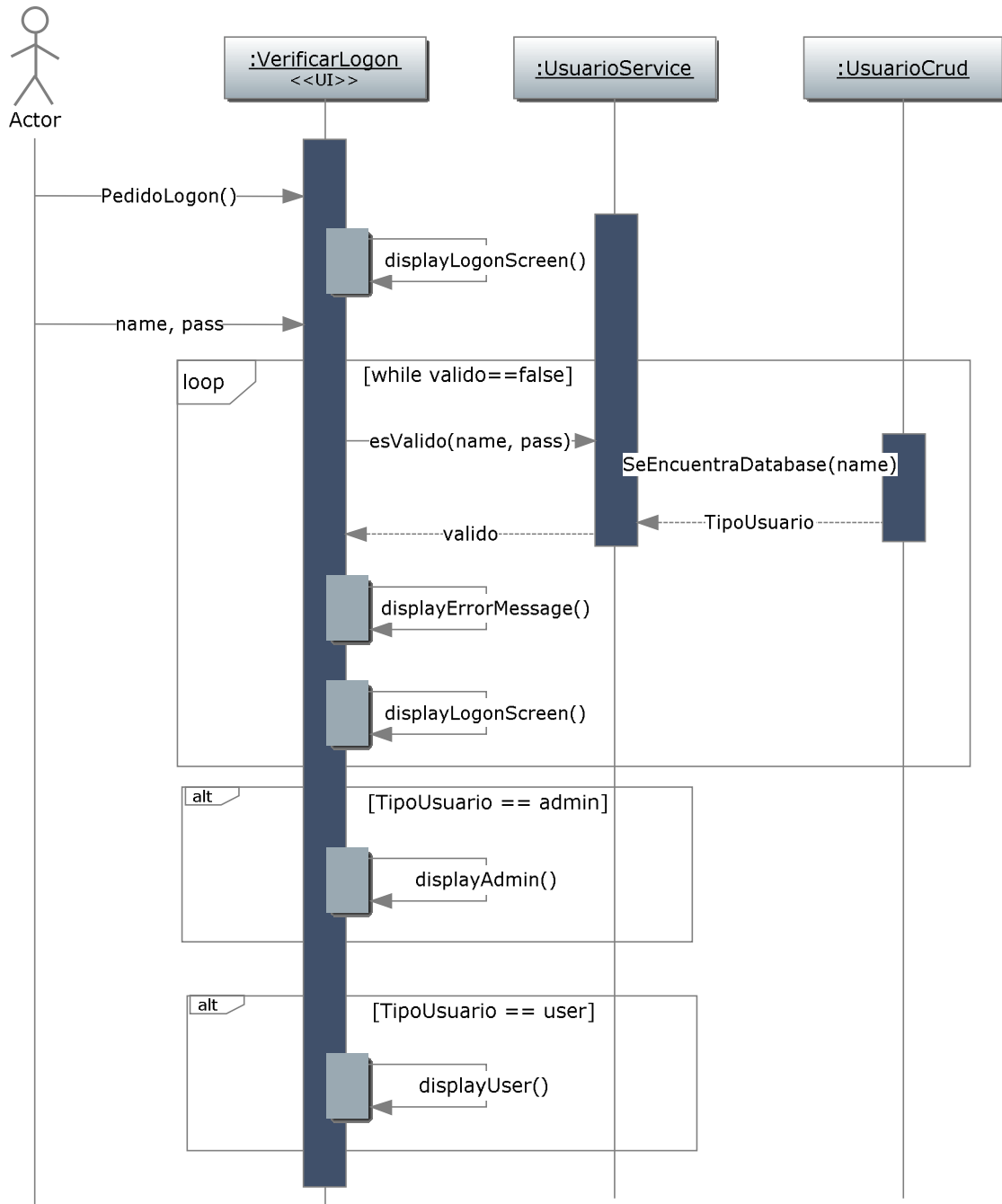
3.2.4 Diagramas de secuencia

UML Diagrama de Paquetes - Encapsulacion



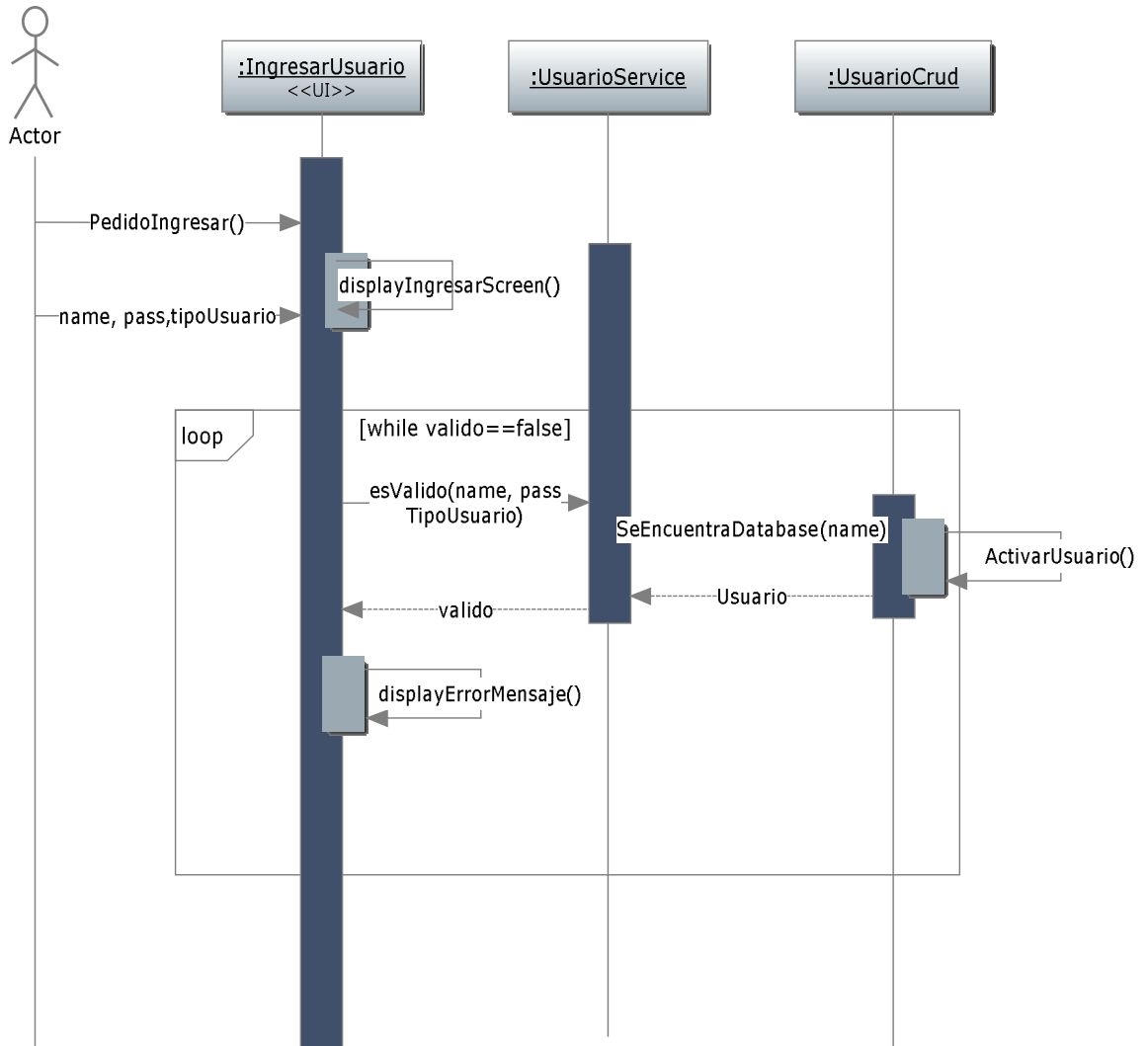


Escenario Log-On



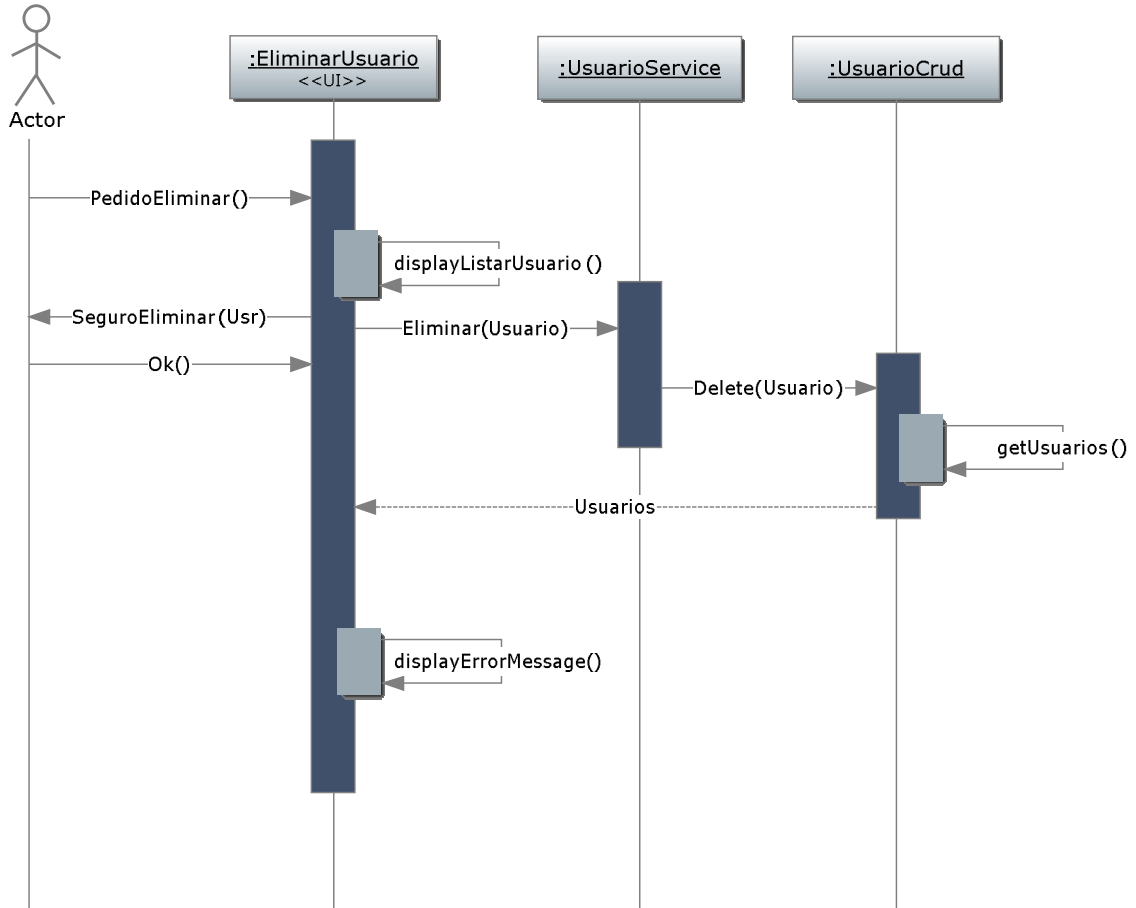


Escenario Ingresar Usuario



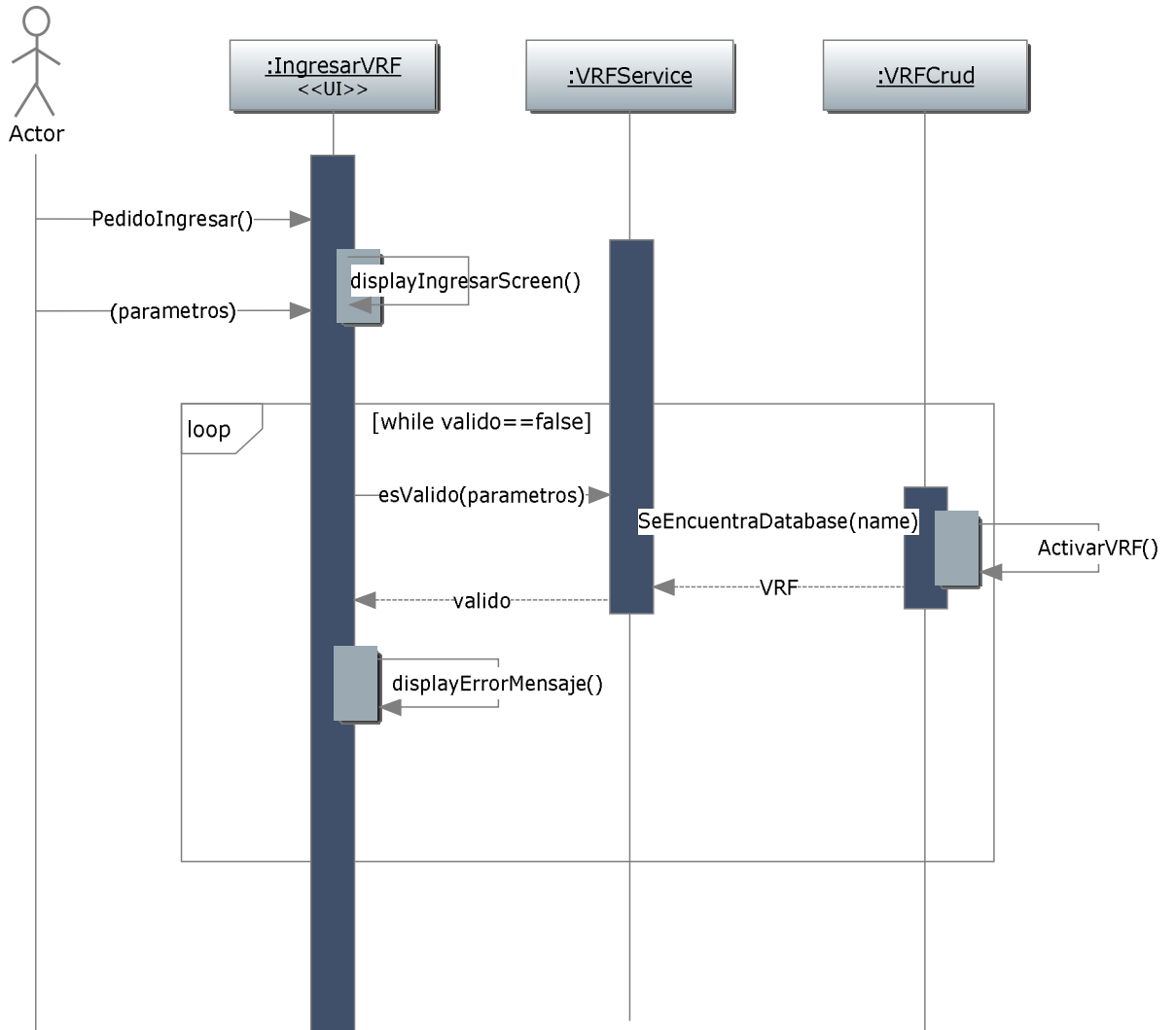


Eliminar Usuario



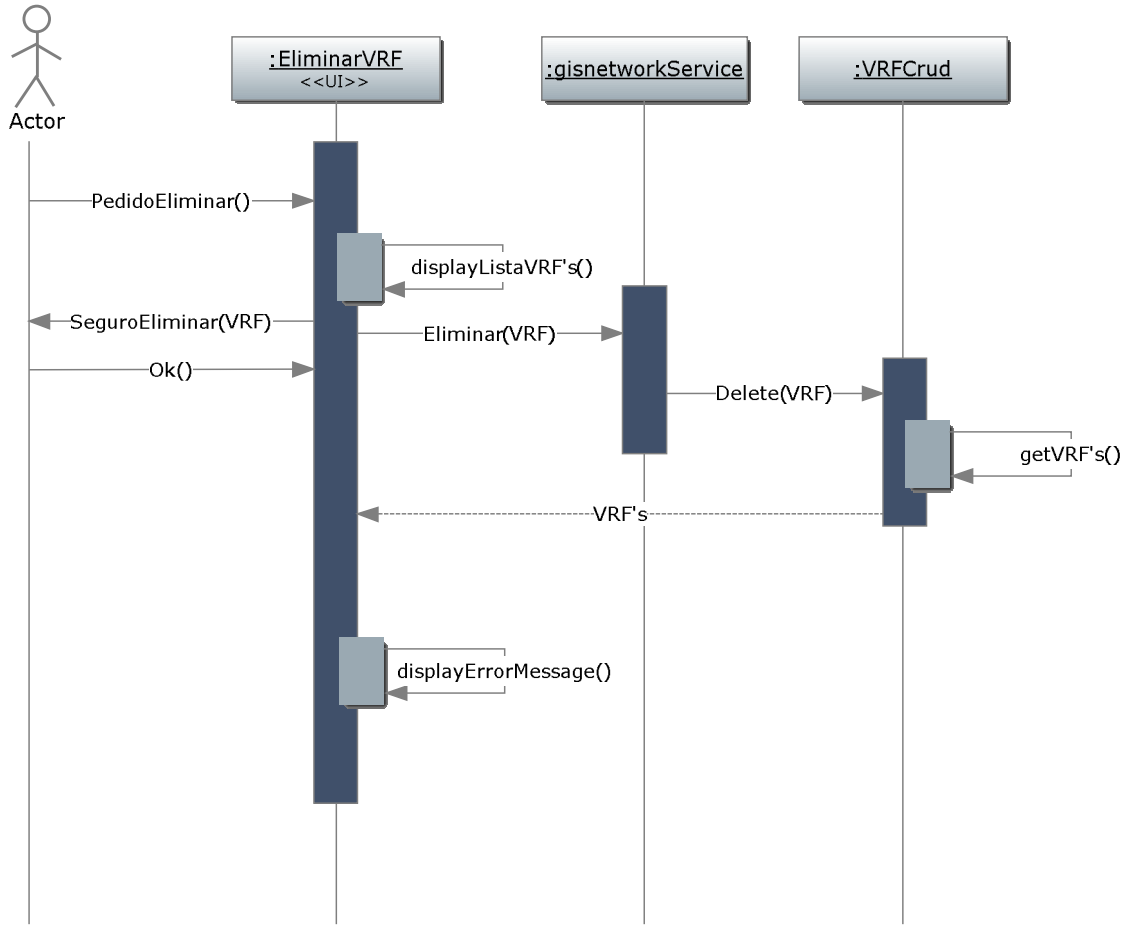


Ingresar VRF



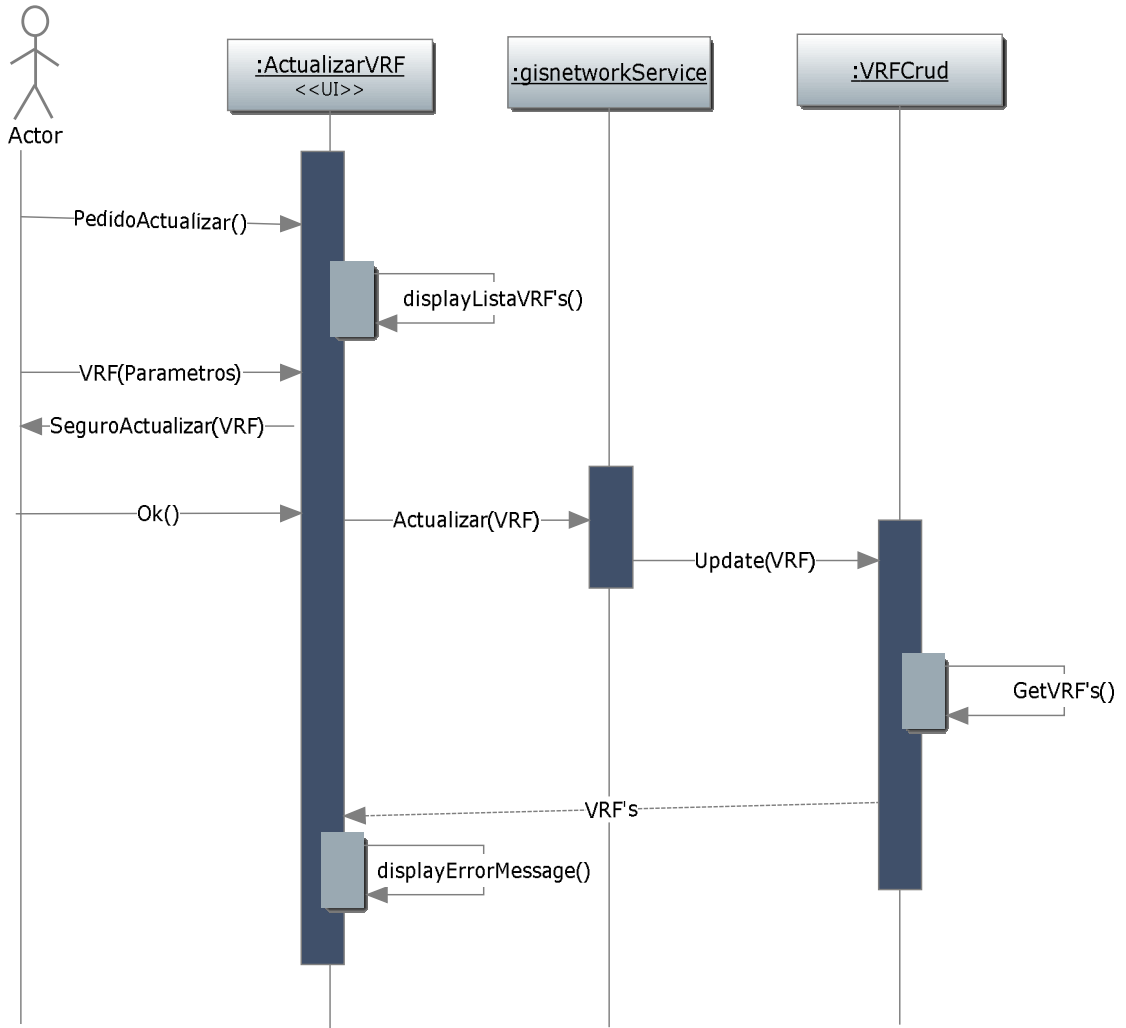


Eliminar VRF



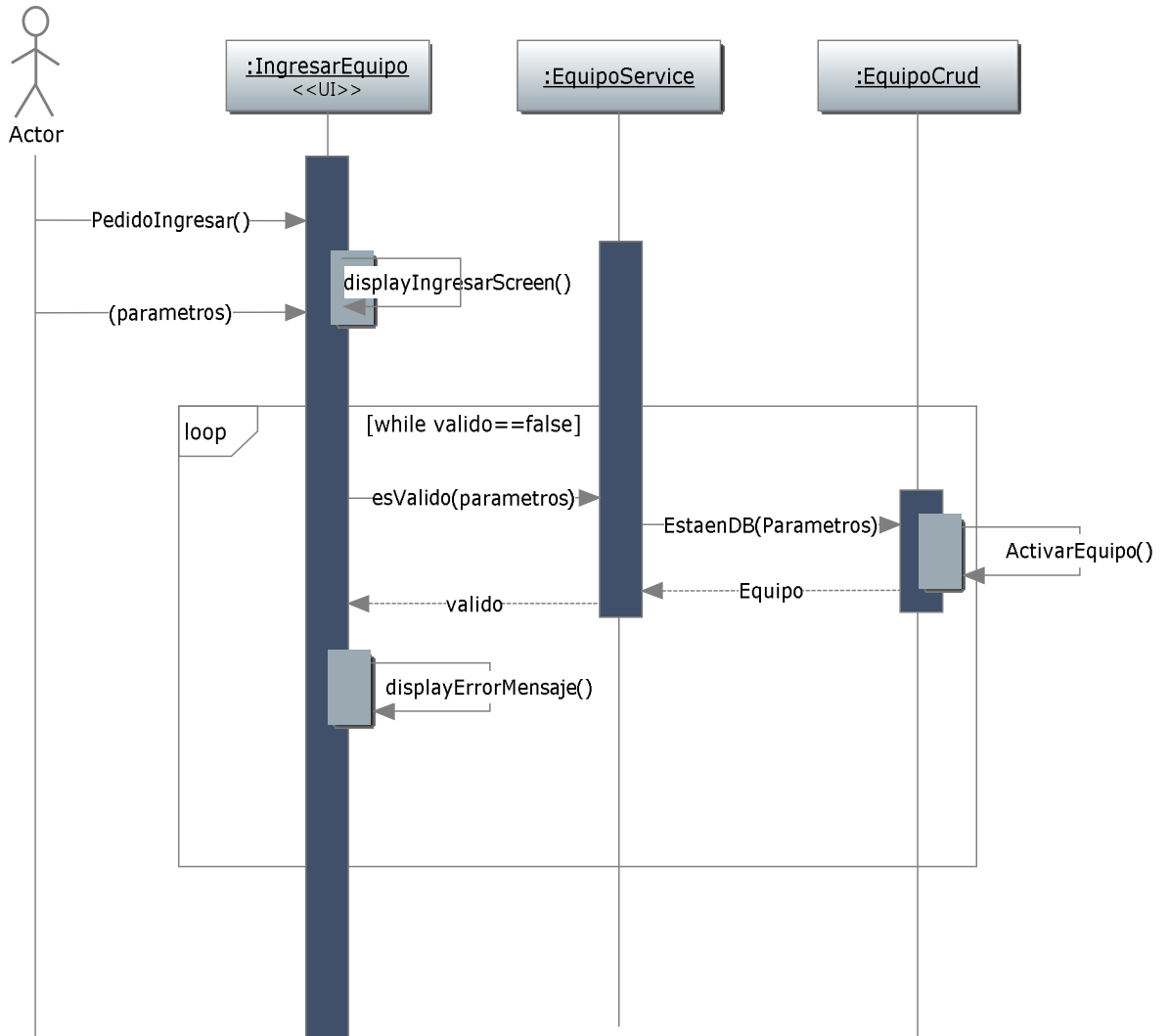


Actualizar VRF



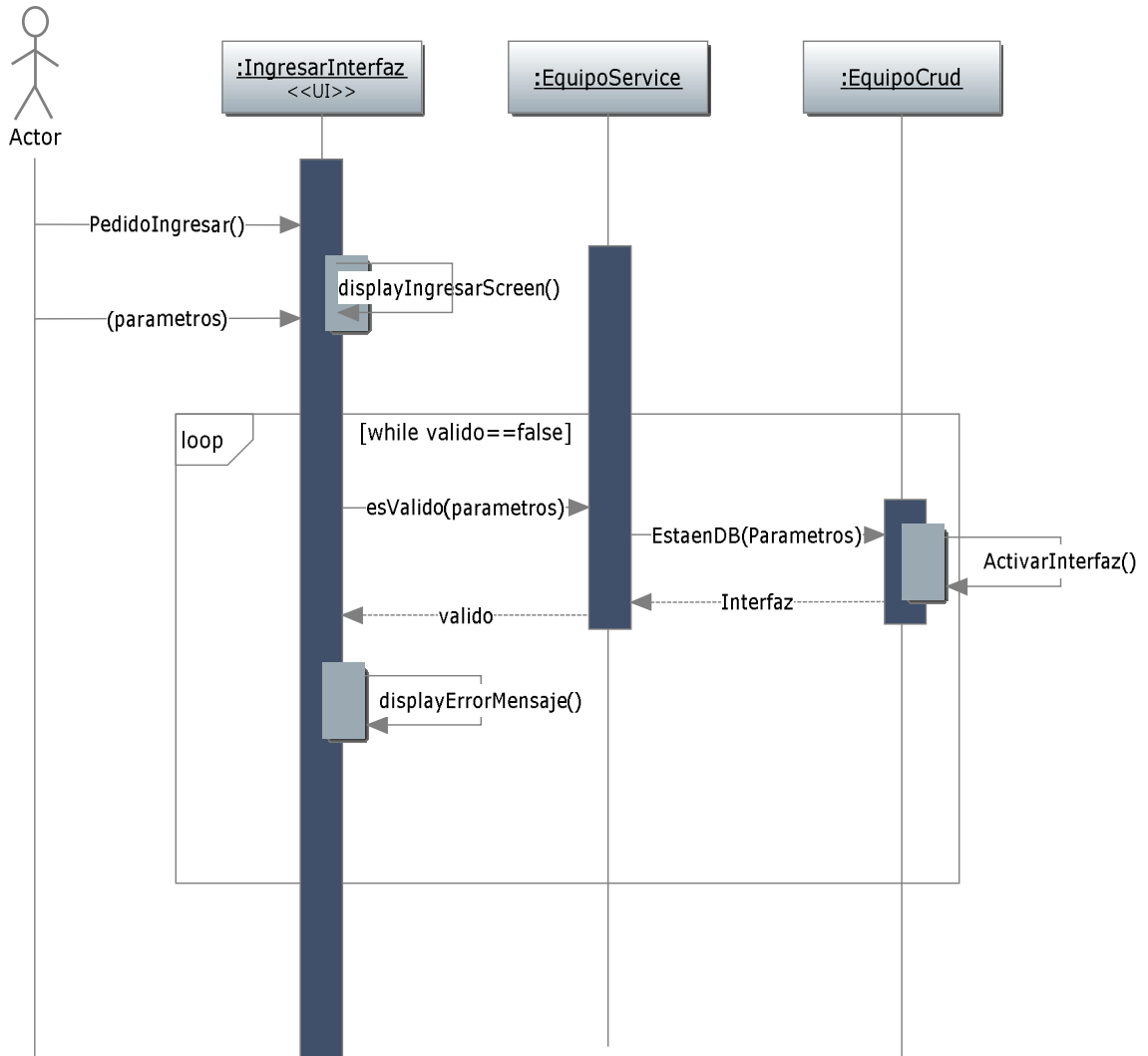


Ingresar Equipo



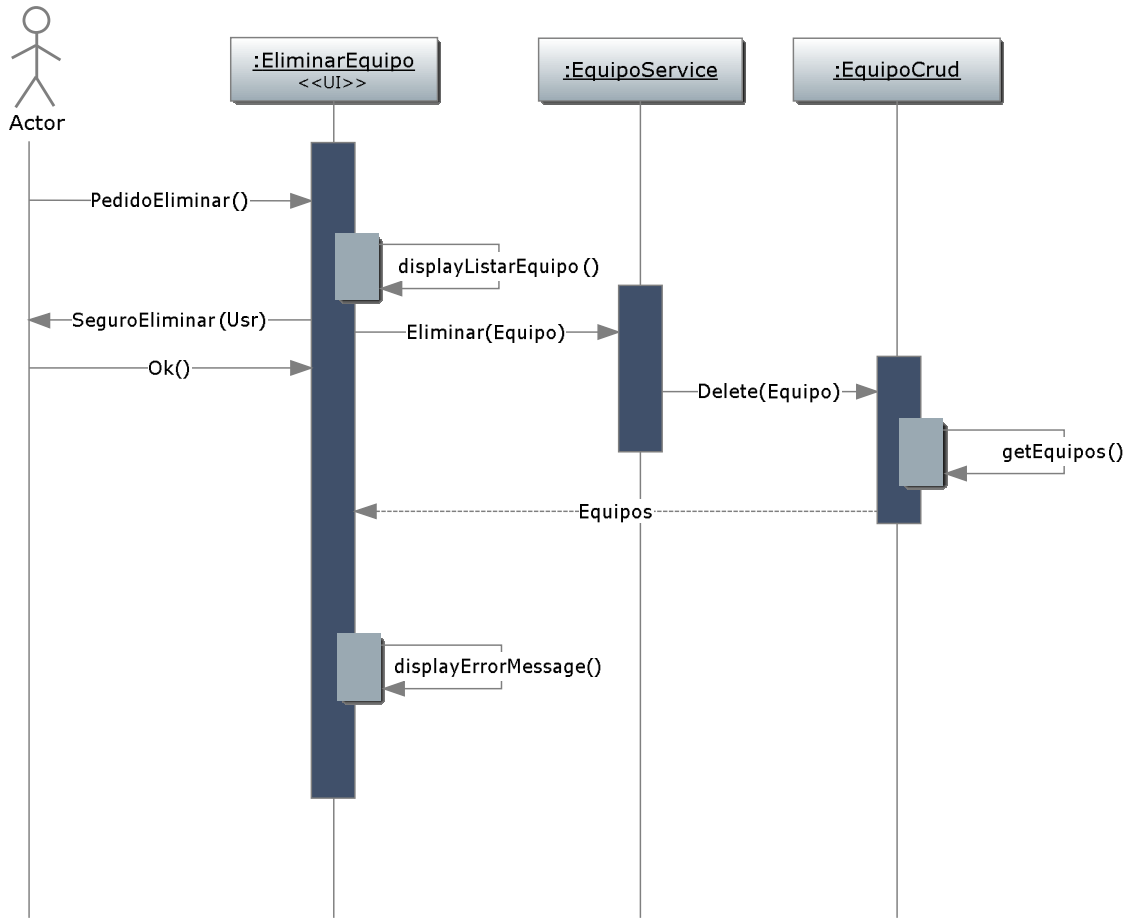


Ingresar Interfaz del Equipo



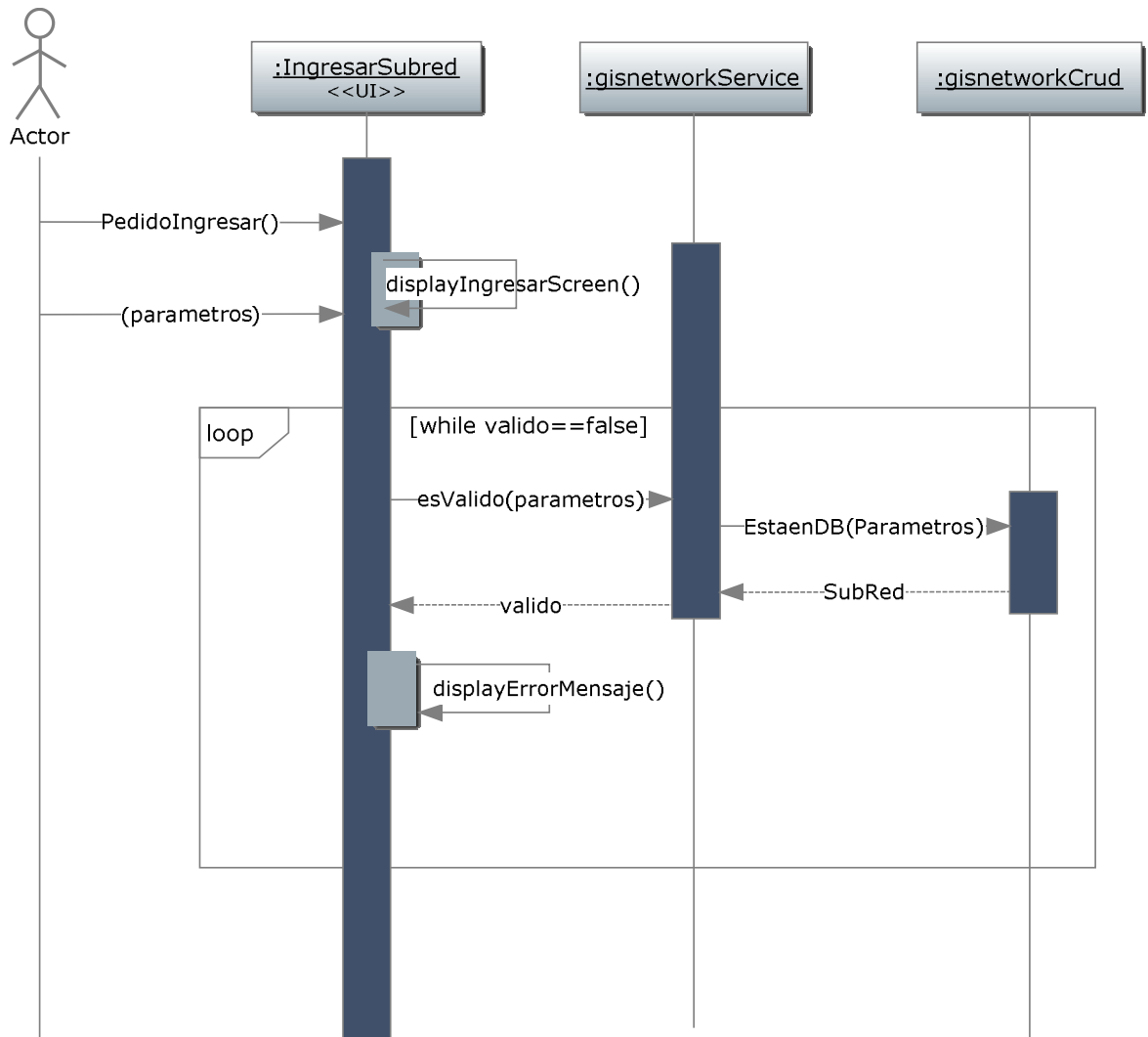


Eliminar Equipo



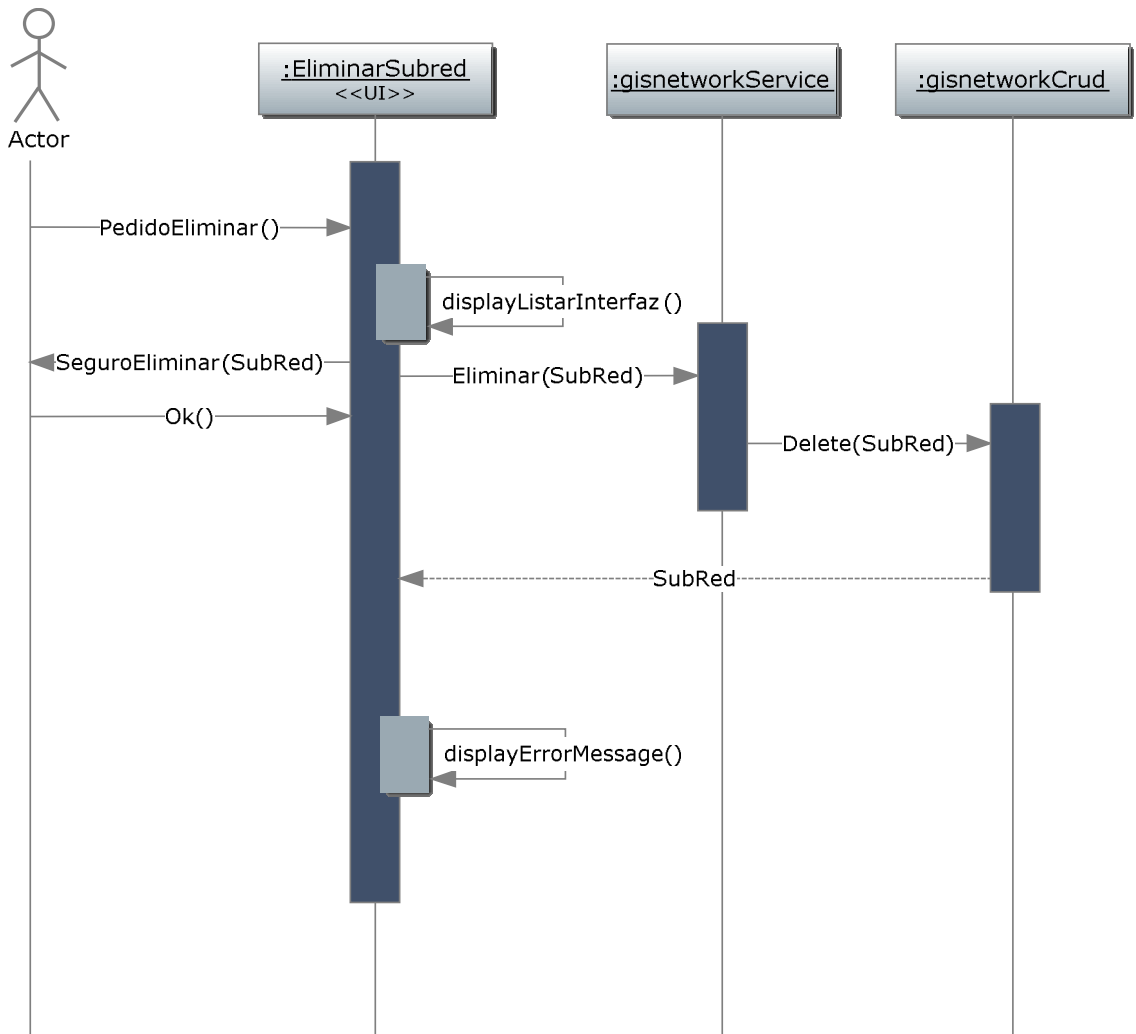


Ingresar Subred



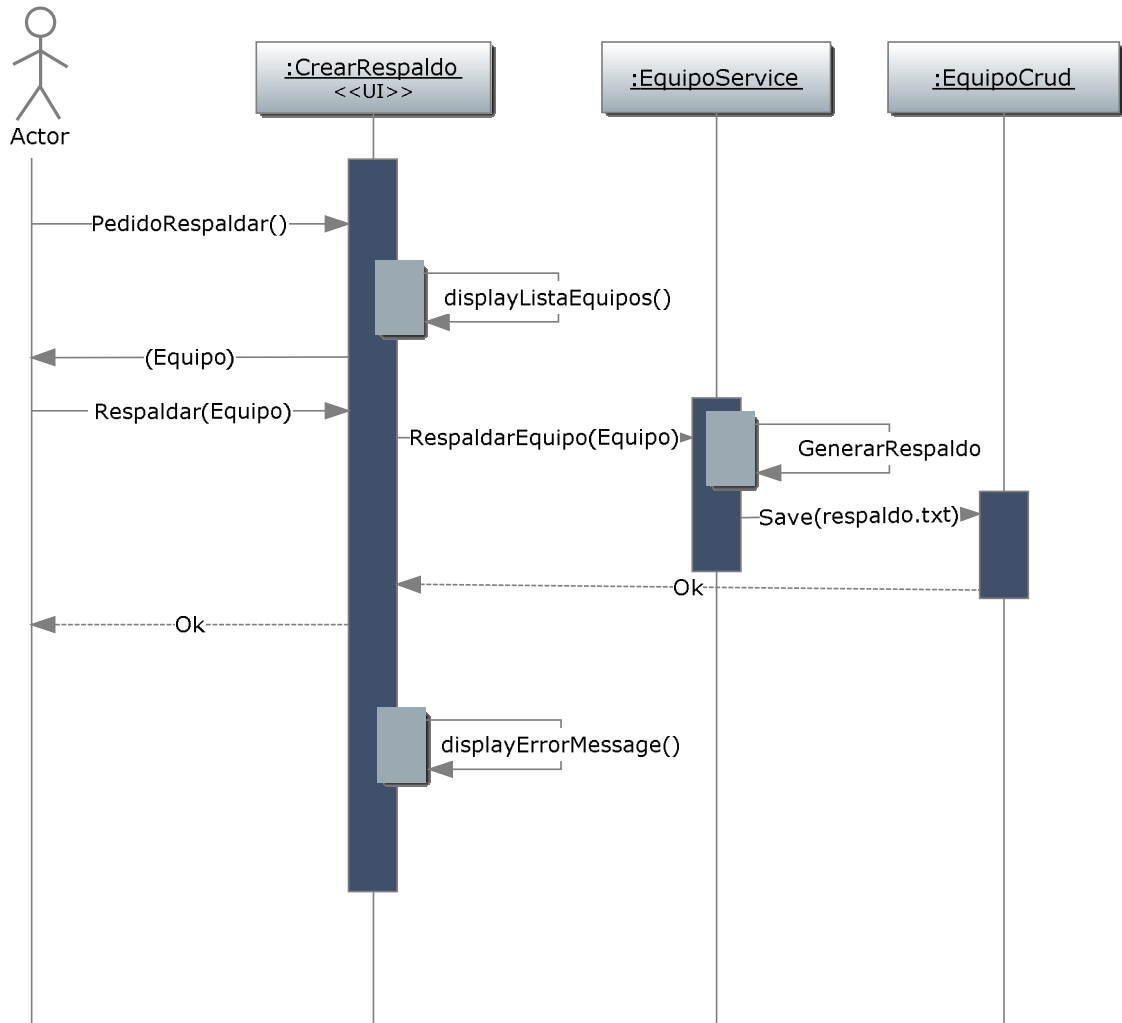


Eliminar Subred



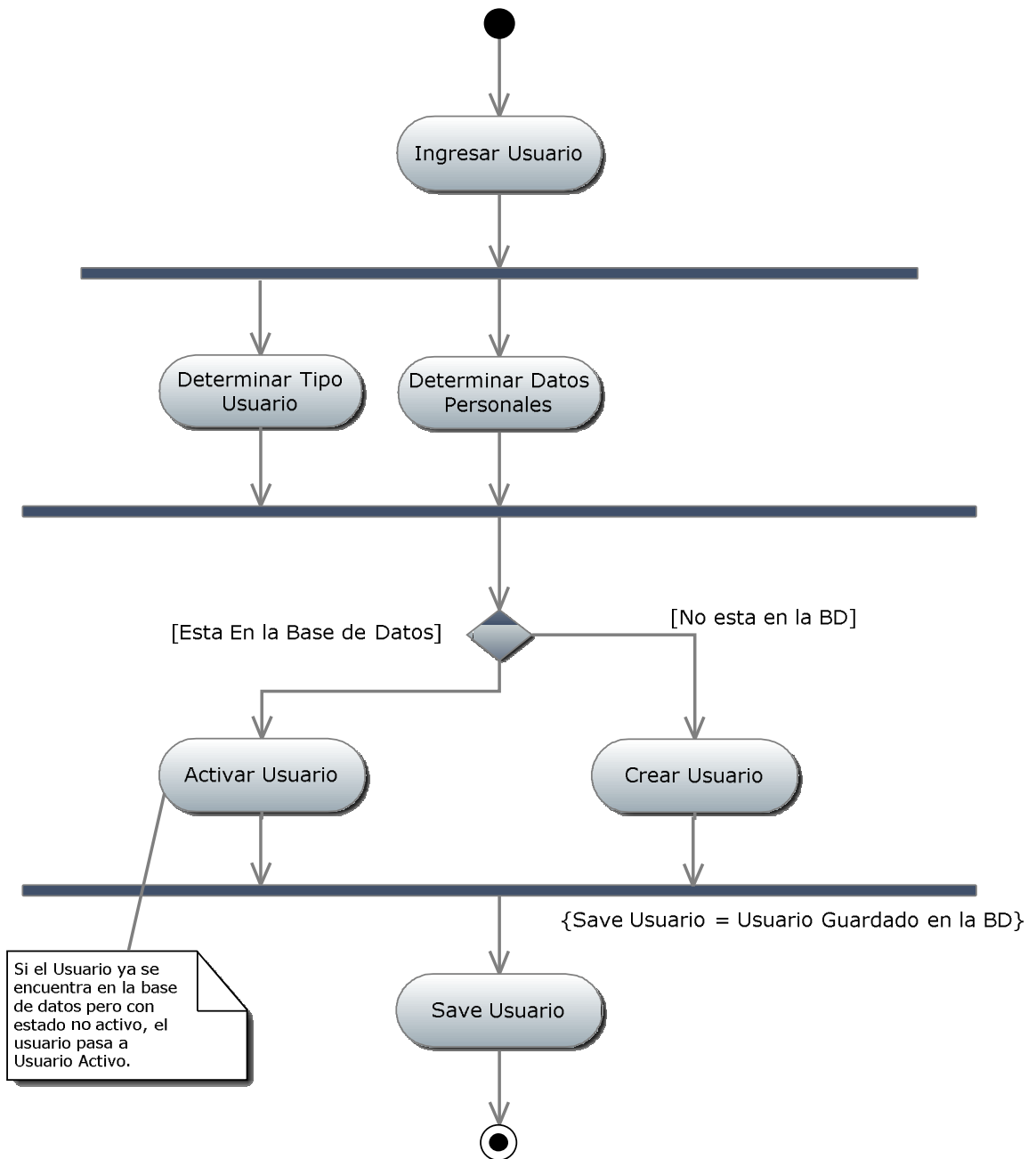


Crear Respaldo Equipo



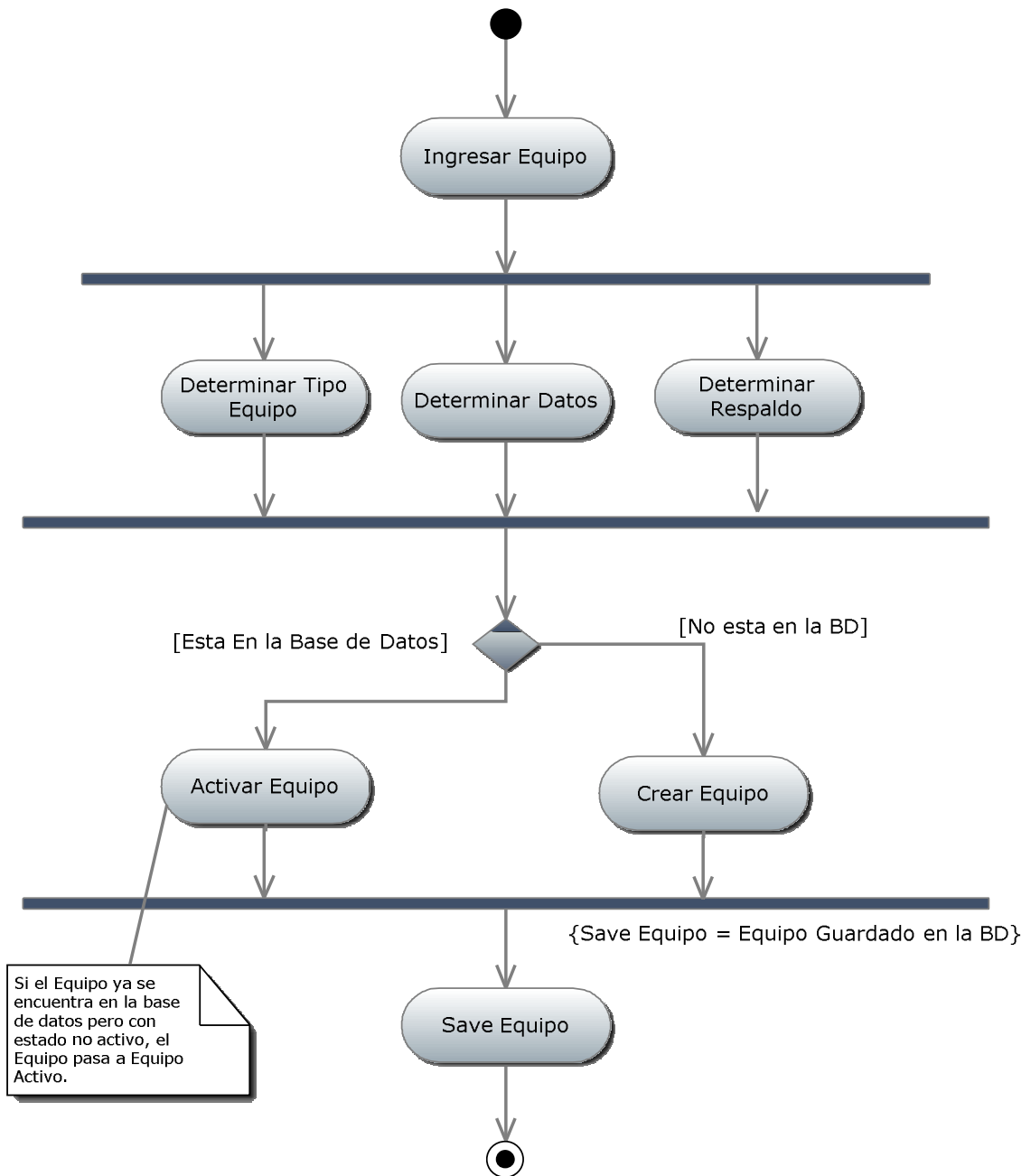


UML Diagrama Actividad: Ingresar Usuario



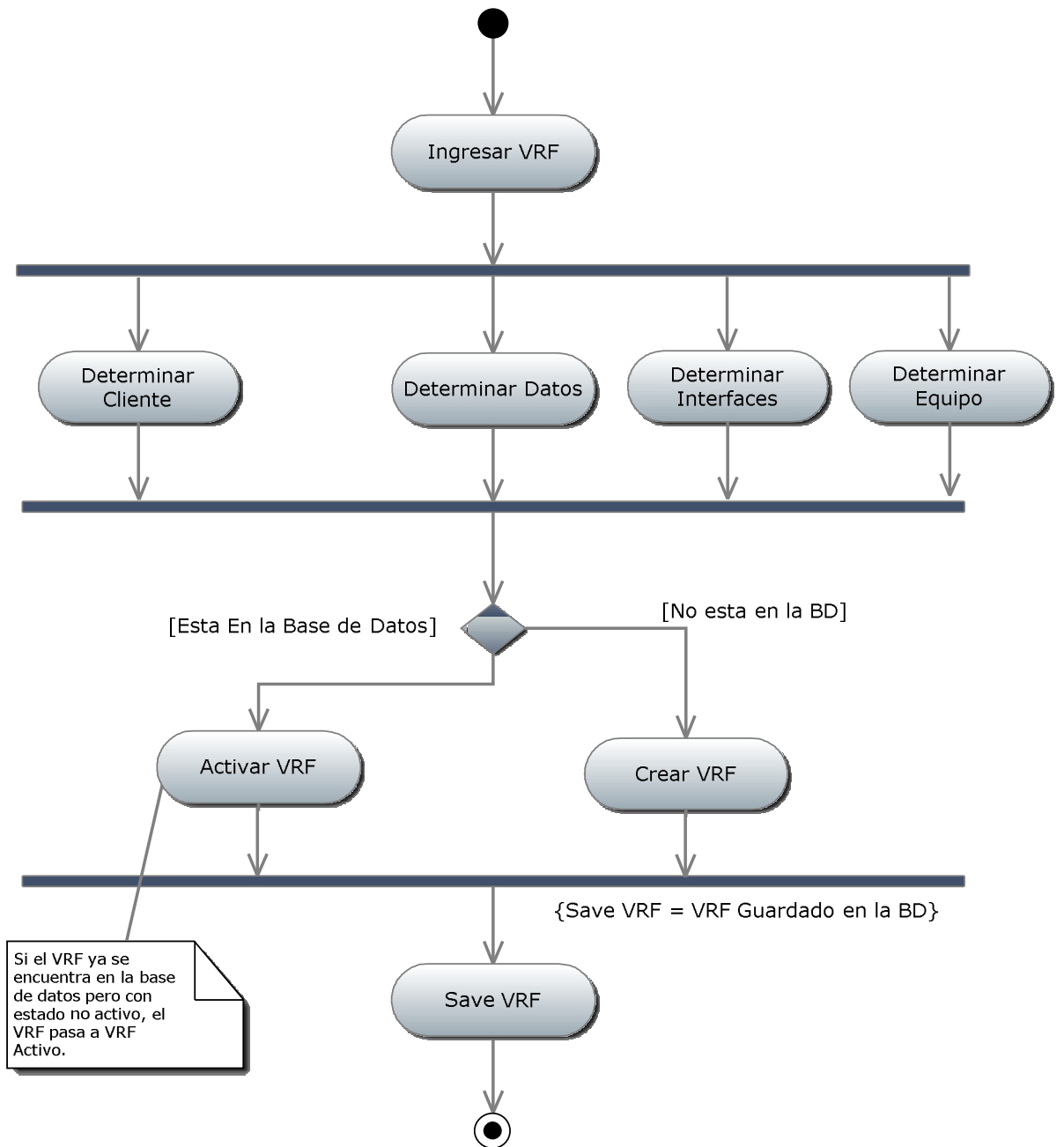


UML Diagrama Actividad: Ingresar Equipo



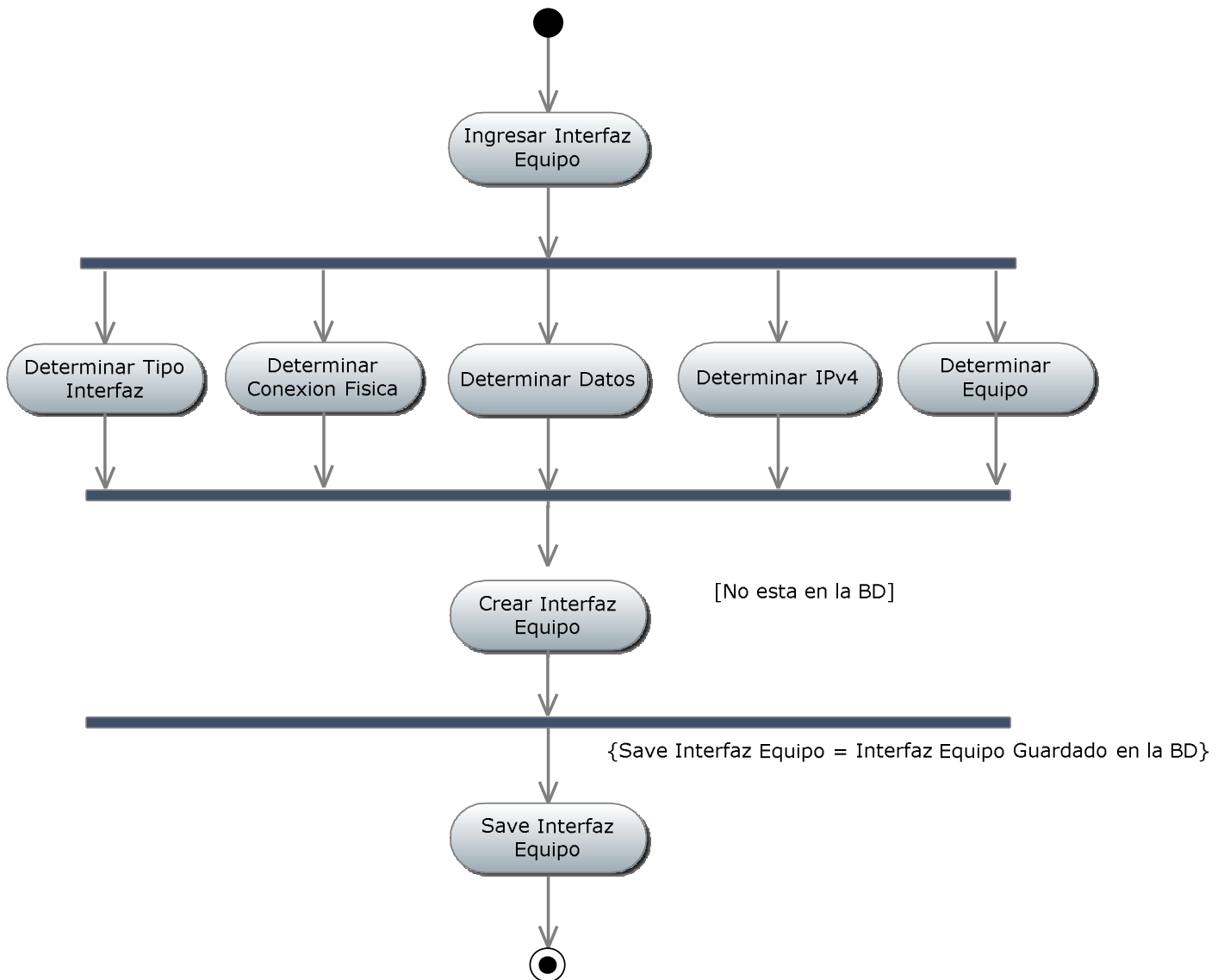


UML Diagrama Actividad: Ingresar VRF



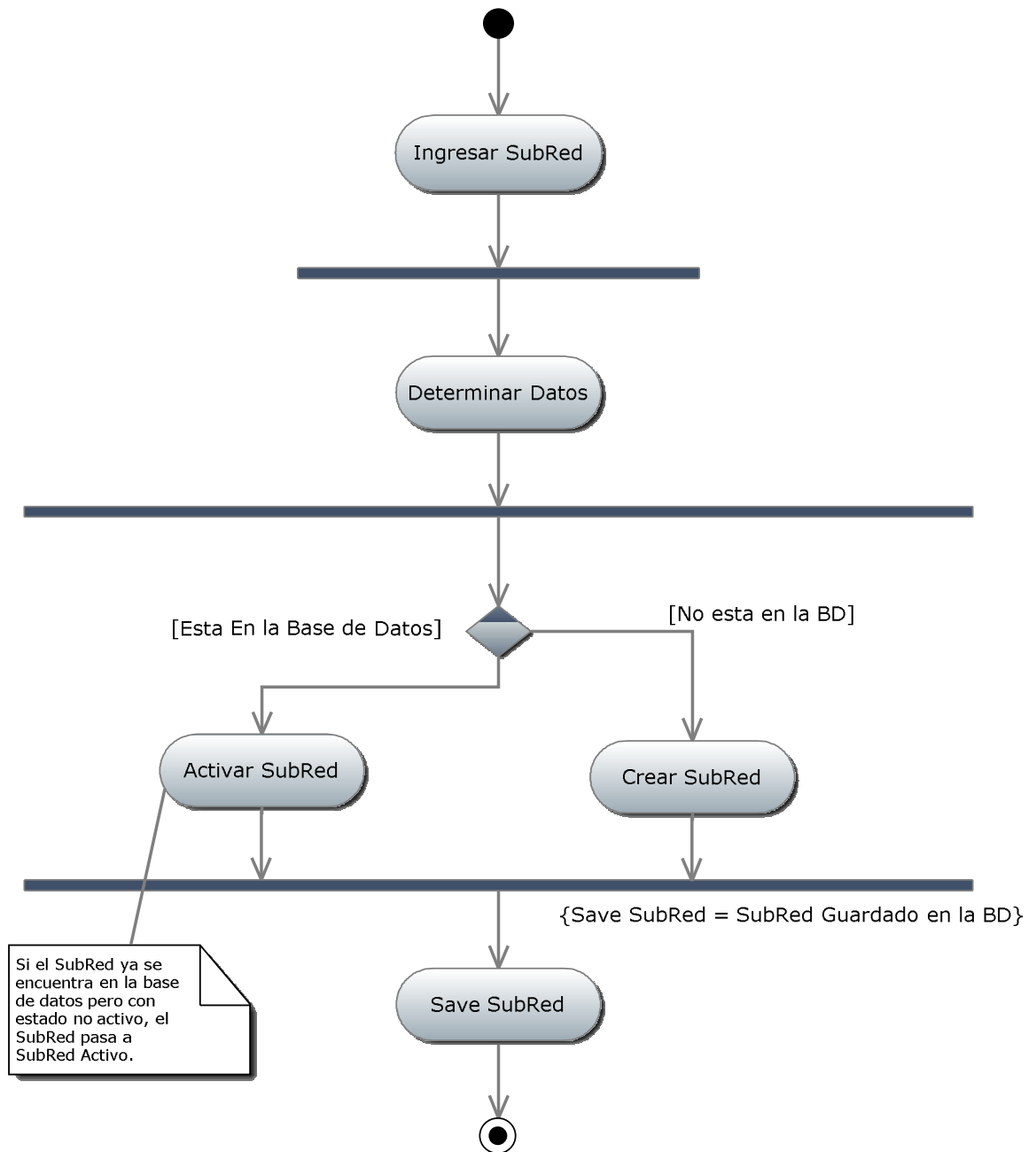


UML Diagrama Actividad: Ingresar Interfaz Equipo



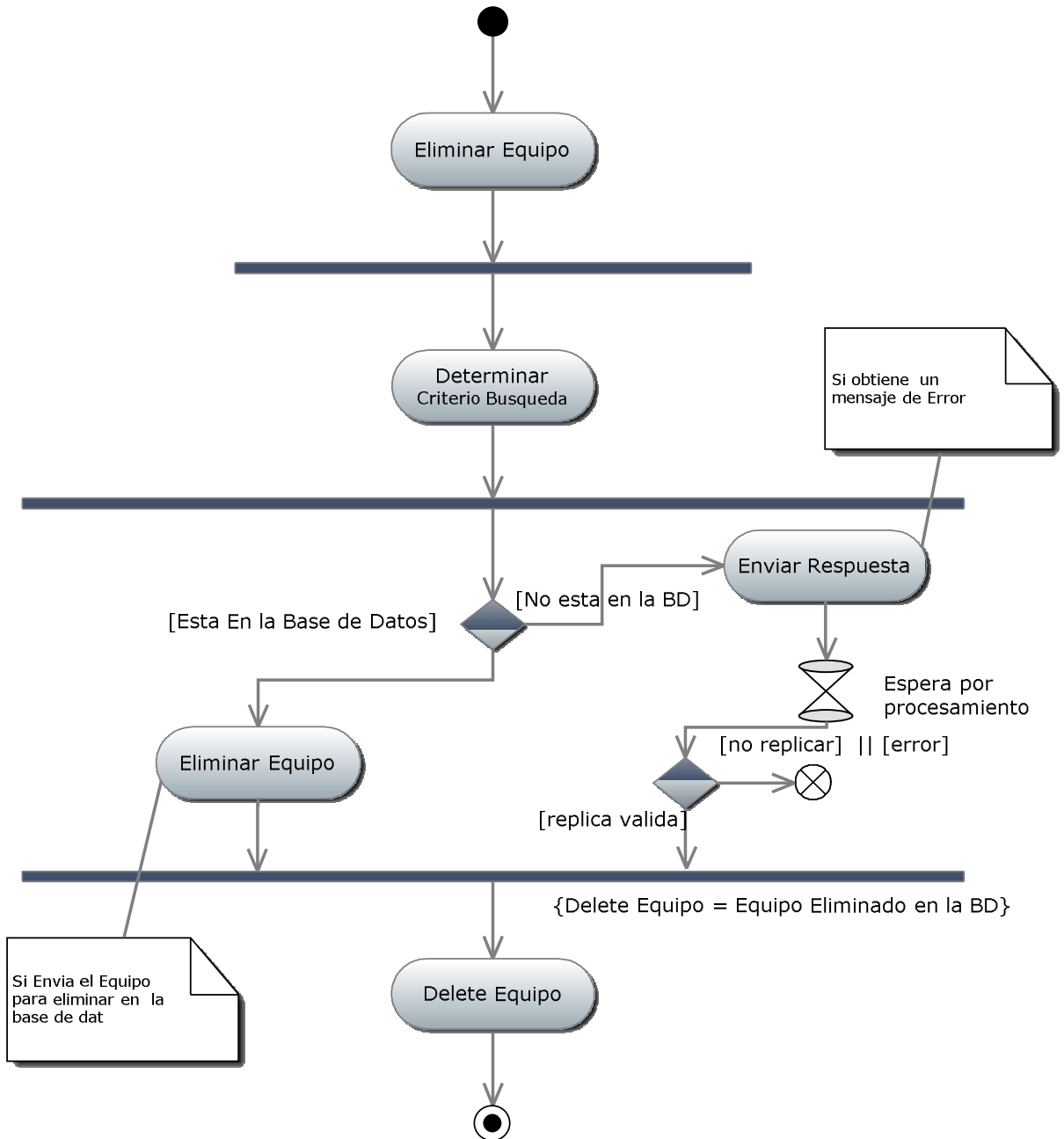


UML Diagrama Actividad: Ingresar SubRed



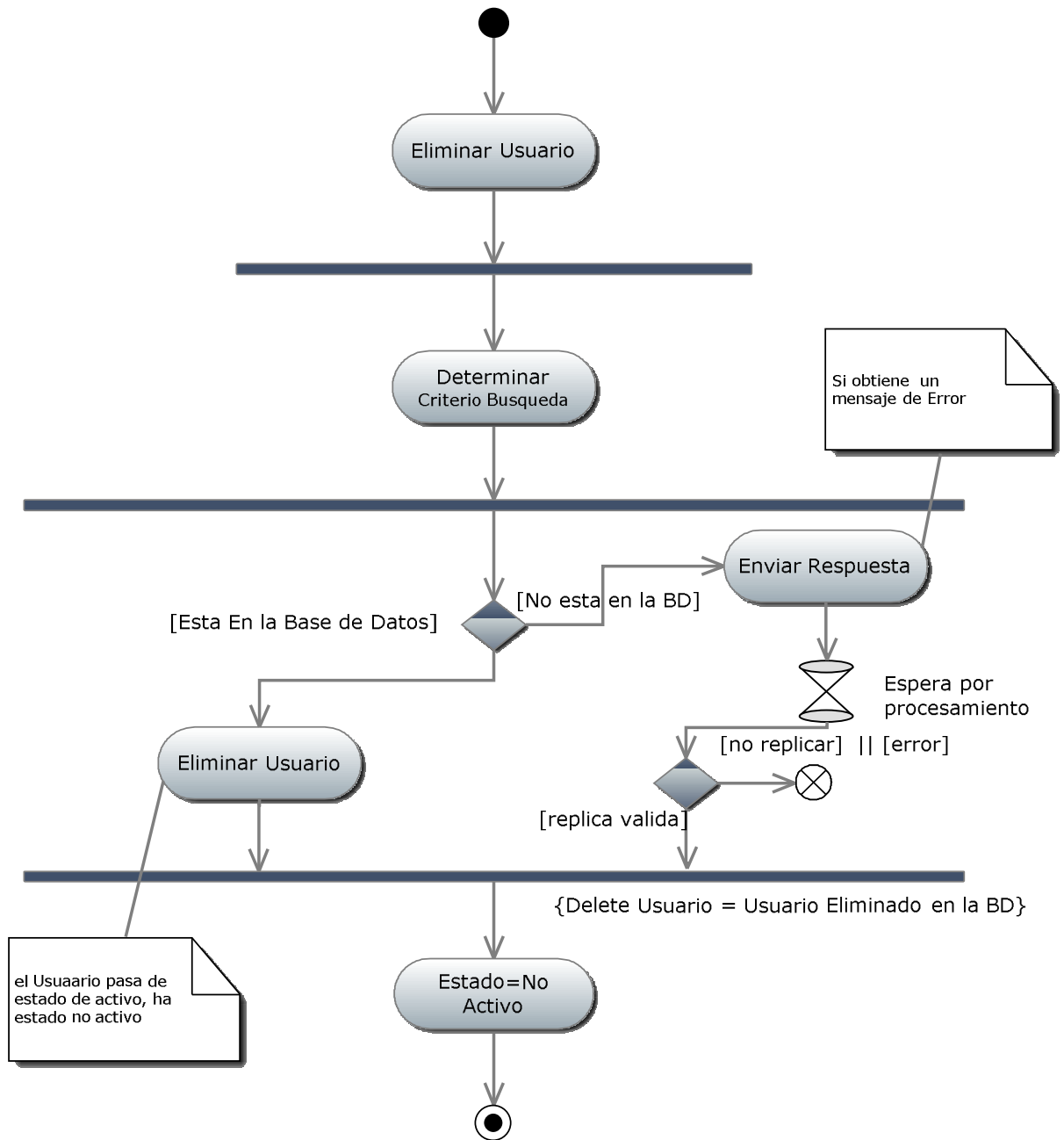


UML Diagrama Actividad: Eliminar Equipo



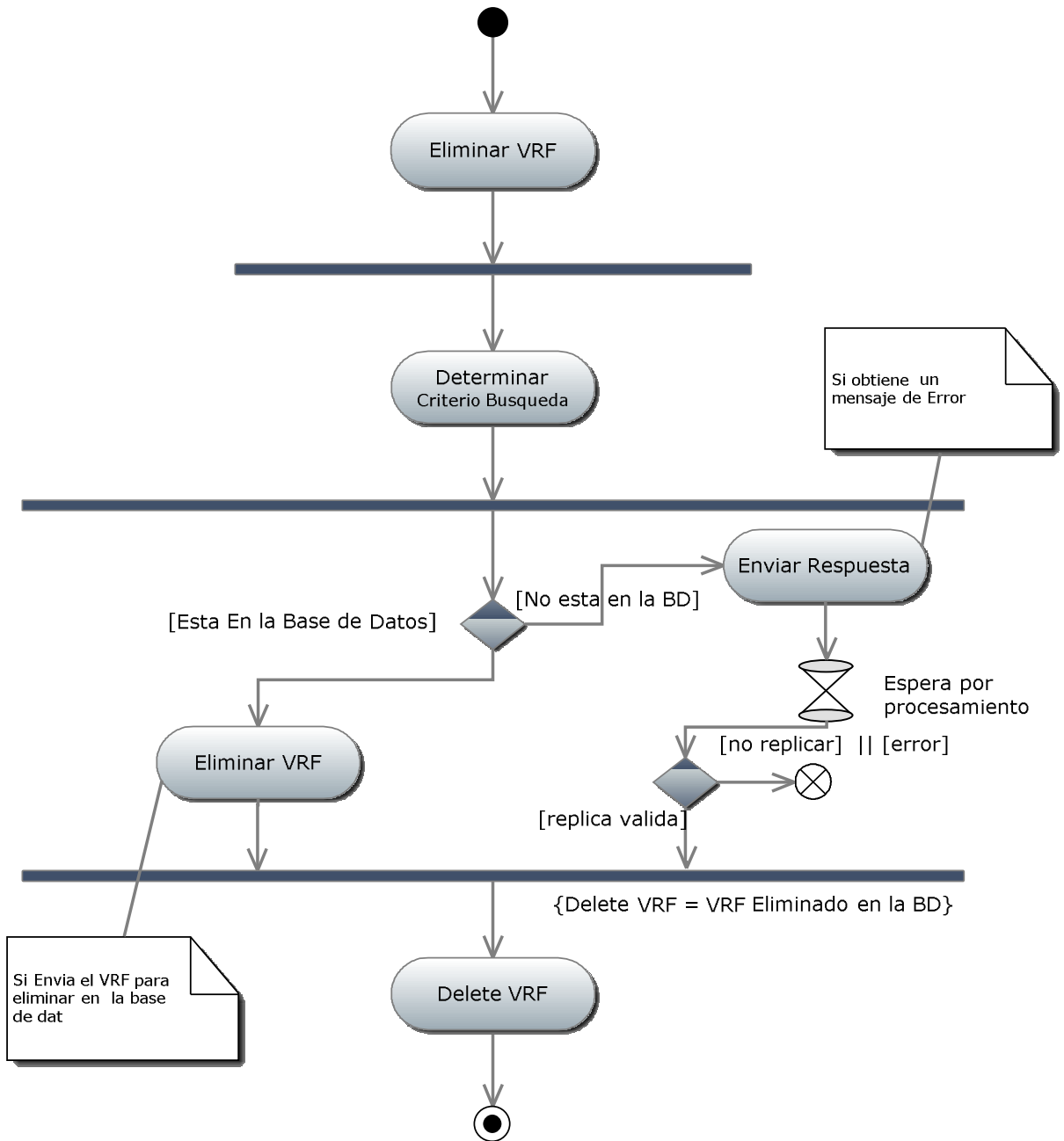


UML Diagrama Actividad: Eliminar Usuario



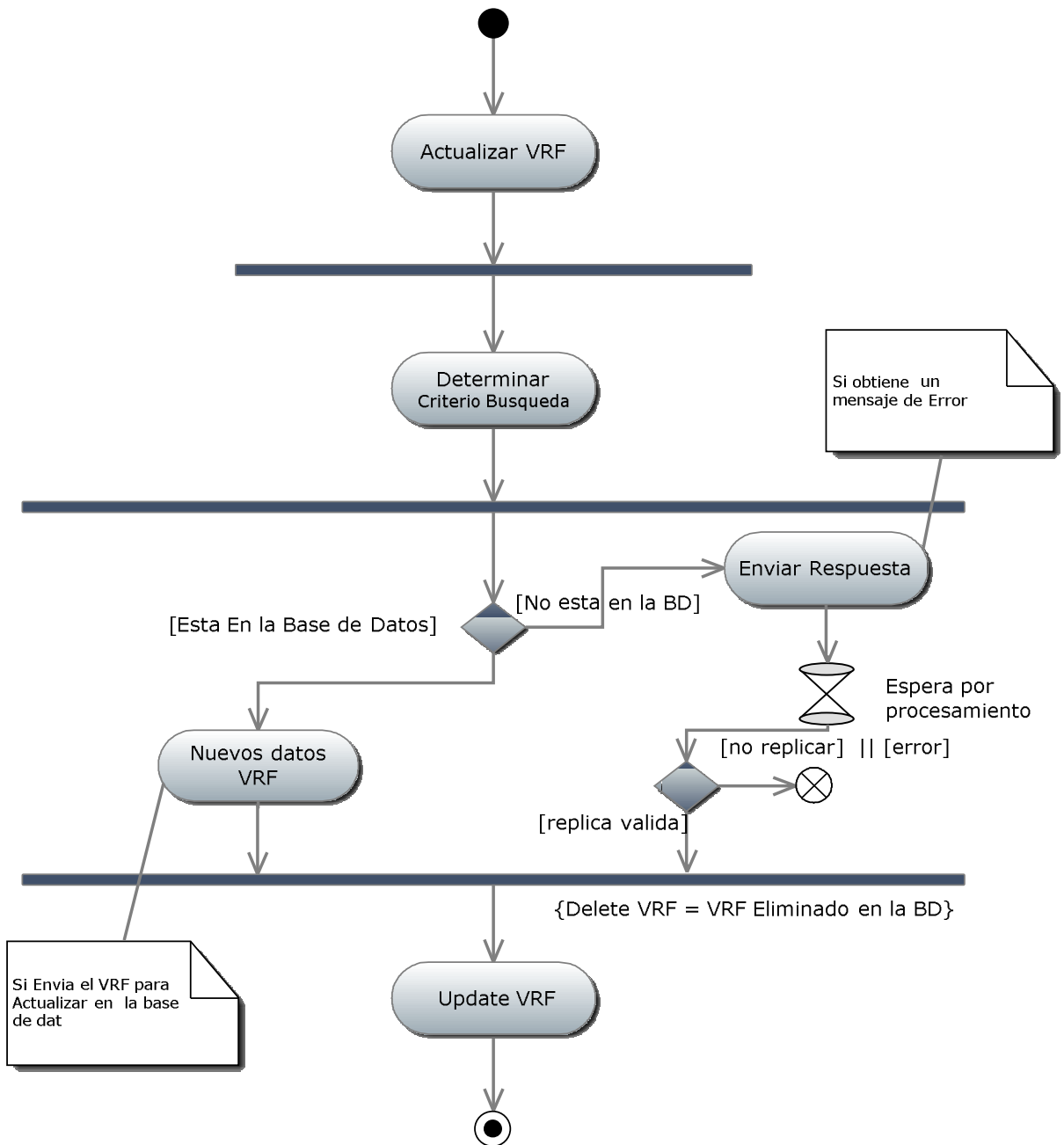


UML Diagrama Actividad: Eliminar VRF



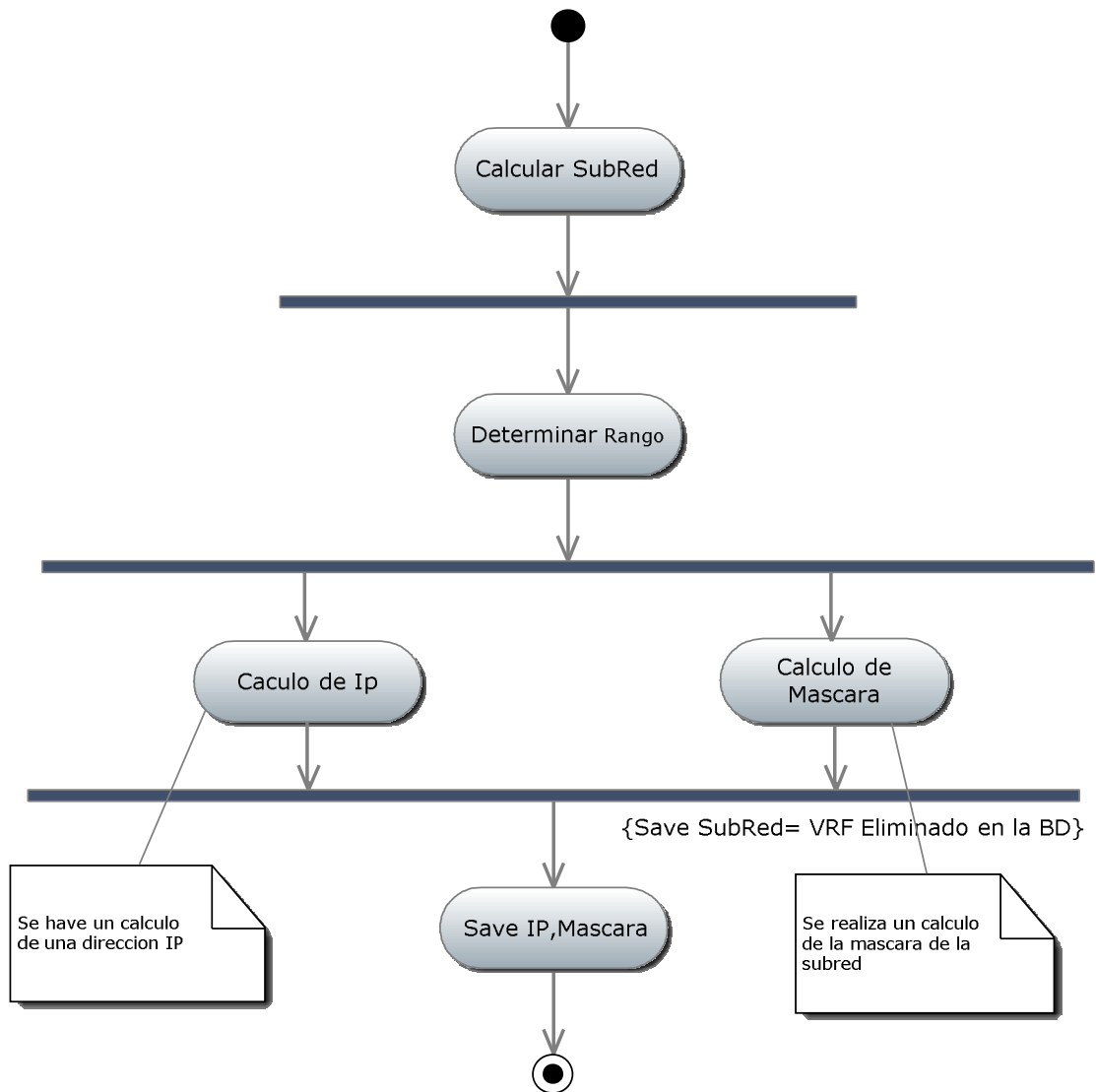


UML Diagrama Actividad: Actualizar VRF



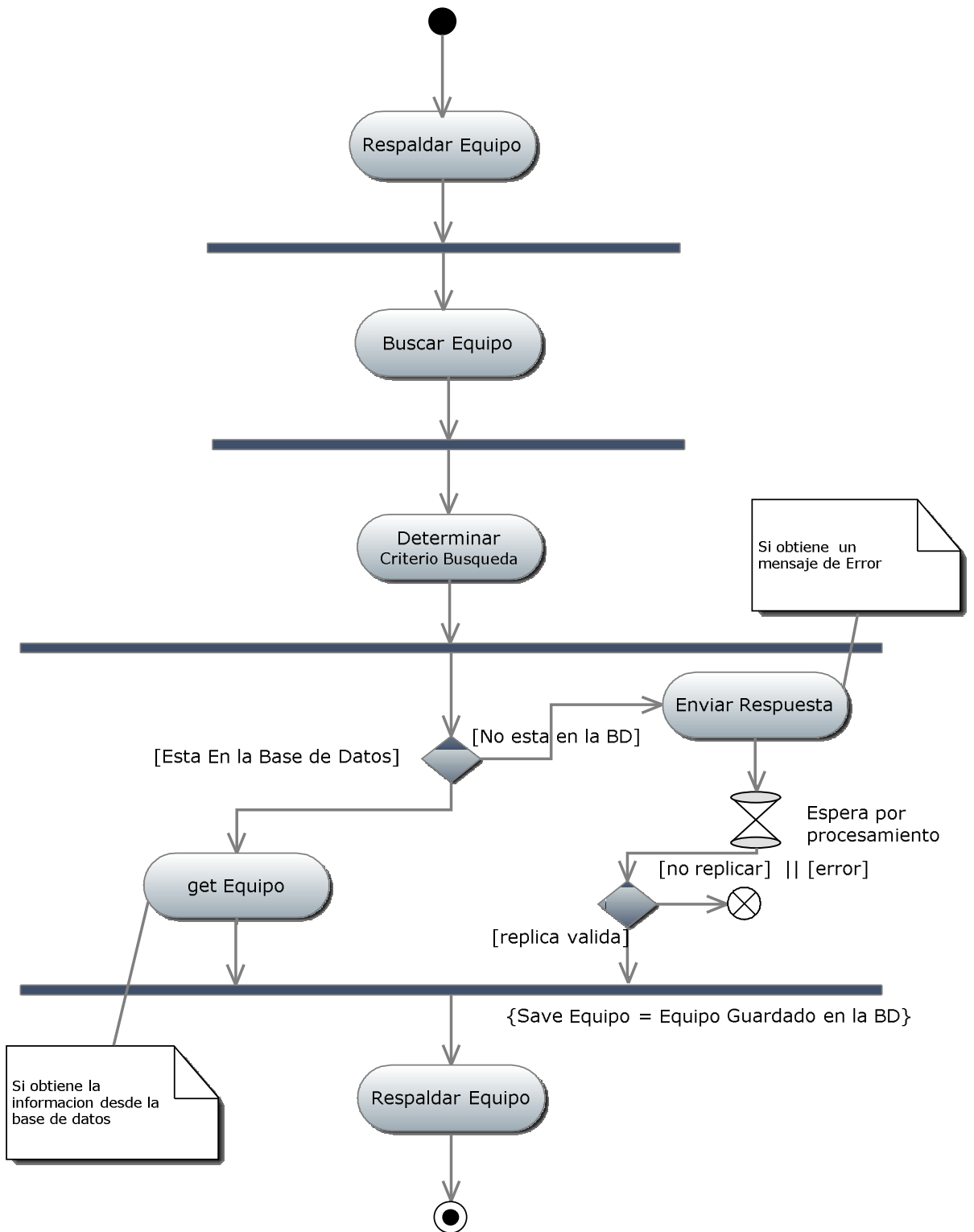


UML Diagrama Actividad: Calcular SubRed





UML Diagrama Actividad: Crear Respaldo Equipo





3.3 IMPLEMENTACIÓN

3.3.1 Modelo de Red IP/MPLS Virtual

Durante la implementación del proyecto se trabajo sobre un modelo estándar para Una red IP/MPLS, Se tomo en consideración que disponga de todos los elementos involucrados en un modelo de red que involucra el uso del protocolo SNMP, evitando complejidades propias de un sistema en producción, pero tomando en cuenta dichos escenarios ya que el sistema se trata de un prototipo.

Se considero un modelo Jerárquico que cuenta con elementos en las tres capas de núcleo, distribución y acceso

A continuación se presenta la topología física que se empleo en la construcción del modelo virtual de red

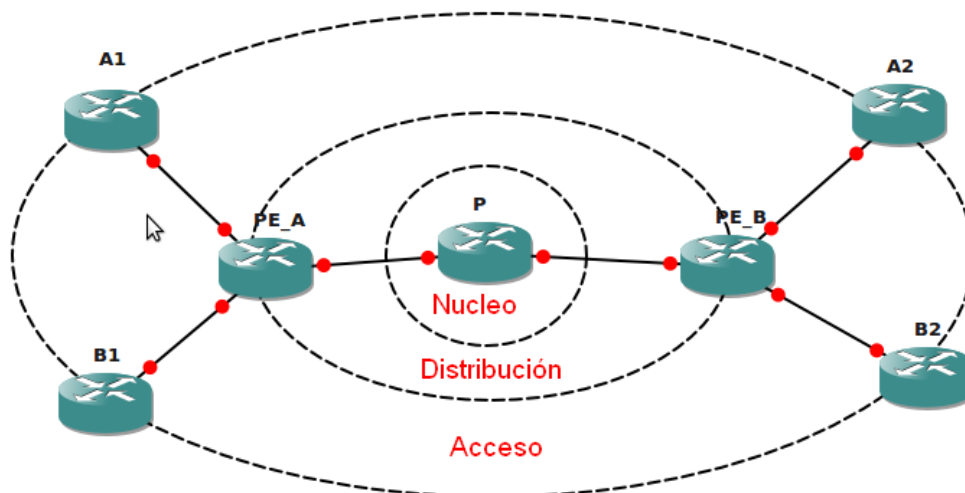


Figura 3.3 Red IP/MPLS Virtual



En la figura anterior observamos el equipo denominado P que representa la capa de core o núcleo del dominio MPLS donde únicamente se gestiona el tráfico mediante el intercambio de etiquetas.

Para la capa de distribución se utilizaron dos nodos denominados PE_A y PE_B por sus características de Provider Edge.

Como IGP se utilizó el protocolo de enrutamiento de estado de enlace OSPF que permite la conectividad entre los equipos que conforman el dominio MPLS

Para las pruebas a realizarse durante el proceso de desarrollo de la aplicación se agregaron cuatro equipos dentro de la Jerarquía de Customer Edge denominados A1, A2, B1, B2. Que representan a los equipos ubicados para brindar acceso a los clientes

Este modelo reúne las características propias de un sistema funcional de IP/MPLS que involucra todos los procesos de configuración que se llevan a cabo en redes que se encuentran en producción y brindan servicios a clientes como la red Centrosur IP/MPLS.

La herramienta que se utilizó para elaborar este esquema es GNS3 que es un simulador de redes que se basa en el IOS de Cisco de modo que proporciona a los usuarios un entorno de trabajo real.

Ya que GNS3 además de ser software de libre uso permite el acceso a su red virtual desde equipos físicos externos reales, como el acceso a máquinas virtuales, por lo que se pueden realizar pruebas en los IOS de los equipos con características similares a los de la red en producción.



3.3.2 Capa de Datos

Diagrama de Base de Datos

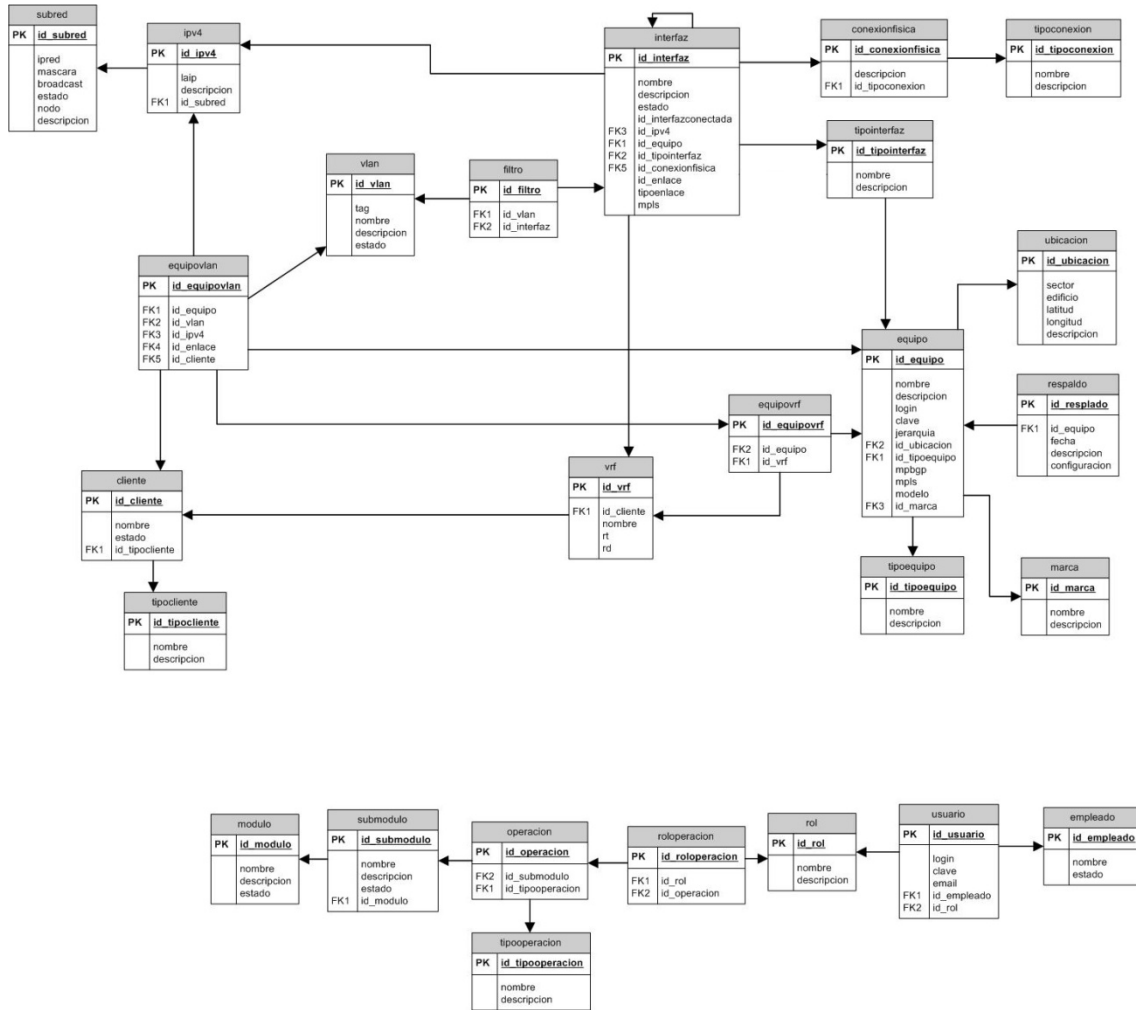


Figura 3.4 Diagrama de Base de Datos

Definición de las tablas de la Base de Datos

CLIENTE

Campo	Tipo	Nulo	Predeterminado	Comentarios	Llave
Id_cliente	Int (11)	No		Identificador único al cliente	PK
Nombre	Varchar (30)	Si	NULL	Campo que almacena el nombre y apellido el	



				cliente	
Estado	Int (11)	Si	NULL	1: cliente activo, 2: cliente eliminado, 0: cliente suspendido	
Id_tipo_cliente	Int (11)	Si	NULL	Identificador del tipo de cliente	
Contrato	Varchar (100)	Si	NULL	Es el código de contrato del cliente	

CONEXIONFISICA

Campo	Tipo	Nulo	Predeterminado	Comentarios	Llave
Id_conexiónfísica	Int (11)	No		Identificador único de la conexión física	PK
descripcion	Varchar (200)	No		Descripción de la conexión física	
Id_tipo_conexión	Int (11)	Si	NULL	Identificador del tipo de conexión física	

EMPLEADO

Campo	Tipo	Nulo	Predeterminado	Comentarios	Llave
Id_empleado	Int (11)	No		Identificador único del empleado	PK
nombre	Varchar (30)	Si	NULL	Nombres y Apellidos del empleado	
estado	Int (11)	Si	NULL		

EQUIPO

Campo	Tipo	Nulo	Predeterminado	Comentarios	Llave
Id_equipo	Int (11)	No		Identificador único del equipo	PK
nombre	Varchar (50)	Si	NULL	Hostname del equipo	



descripción	Varchar(200)	Si	NULL	Descripción particular del equipo	
login	Varchar (30)	Si	NULL	Login del usuario administrador del equipo	
clave	Varchar (30)	Si	NULL	Clave del usuario administrador del equipo	
jerarquía	Varchar (30)	No		P,PE,CE. Dependiendo de la jerarquía del equipo	
Id_ubicacion	Int (11)	Si	NULL		
Id_tipo equipo	Int (11)	Si	NULL		
mpbgp	Int (11)	Si	NULL	Variable informativa: 1 mpbgp activado, 0 mpbgp no activado	
mpls	Int (11)	Si	NULL	Variable informativa: 1 mpls activado en modo global, 0 mpls no activado	

EQUIPOVLAN

Campo	Tipo	Nulo	Predeterminado	Comentarios	Llave
Id_equipo vlan	Int (11)	No		Identificador único de la vlan aplicada en un equipo	PK
Id_equipo	Int(11)	No		Identificador del equipo donde esta aplicada la vlan	
Id_vlan	Int (11)	No		Identificador de la vlan aplicada en el equipo	
Id_ipv4	Int (11)	Si	NULL	Identificador del direccionamiento ip de la vlan	



				aplicada en el equipo	
Id_enlace	Int (11)	Si	NULL	Identificador del vrf aplicada en la vlan de un equipo en particular	

EQUIPOVRF

Campo	Tipo	Nulo	Predeterminado	Comentarios	Llave
Id_equipo vrf	Int (11)	No		Identificador único de la vrf aplicada en un equipo	PK
Id_equipo	Int(11)	No		Identificador del equipo donde se ha aplicado una vrf en particular	
Id_vrf	Int (11)	No		Identificador de la vrf aplicada en el equipo	

FILTRO

Campo	Tipo	Nulo	Predeterminado	Comentarios	Llave
Id_filtro	Int (11)	No		Identificador único del filtro aplicado en el interfaz o puerto de un equipo	PK
Id_vlan	Int(11)	Si	Null	Identificador de la vlan que ha sido filtrada en un puerto en un equipo en particular	
Id_interfaz	Int (11)	Si	Null	Identificador de la interfaz o puerto de un equipo al cual se le ha aplicado un filtro de una vlan	

**INTERFAZ**

Campo	Tipo	Nul o	Predeterminad o	Comentarios	Llav e
Id_interfaz	Int (11)	No		Identificador único de una interfaz o puerto de un equipo	PK
nombre	Varchar(30)	No		Nombre de la interfaz o puerto	
descripción	Varchar(200)	Si	NULL	Descripción particular de la interfaz o puerto	
estado	Int (11)	No		Estado de la interfaz	
Id_interfaz conetada	Int (11)	Si	NULL	identificador de la interfaz a la cual esta interconectada	
Id_ipv4	Int (11)	Si	NULL	identificador de la ip de la interfaz	
Id_equipo	Int (11)	No		identificador del equipo al que pertenece la interfaz	
Id_tipointerfaz	Int (11)	Si	NULL	identificador del tipo de interfaz	
Id_conexionfisica	Int (11)	Si	NULL	Identificador de la conexión física entre dos interfaces de equipos	
Id_enlace	Int (11)	Si	NULL	Este es el id ya sea de la tabla vrf o atom	
tipo enlace	Int (11)	Si	NULL	3=vrf; 2=atom	
mpls	Int (11)	Si	NULL	1-mpls activado, 0-	



				mpls no activado y no forma parte de dominio mpls, 4-la interfaz forma parte del dominio mpls pero no tiene mpls activado	
--	--	--	--	---	--

IPV4

Campo	Tipo	Nulo	Predeterminado	Comentarios	Llave
Id_ipv4	Int (11)	No		identificador único de una dirección ipv4 aplicada en una interfaz de un equipo	PK
laip	Varchar (20)	No		dirección ipv4	
descripción	Varchar (100)	Si	NULL	Descripción particular de la dirección ip de la interfaz	
Id_subred	Int(11)	Si	NULL	identificador de la subred dentro de cuyo rango pertenece a la ip	

RESPALDO

Campo	Tipo	Nulo	Predeterminado	Comentarios	Llave
Id_respaldo	Int (11)	No		Identificador único del respaldo de un equipo	PK
Id_equipo	Int (11)	Si	NULL	identificador único de un equipo que ha sido respaldado	
fecha	Date time	Si	NULL	fecha en la	



				que se realizo el respaldo, formato: yyyy-MM-dd-HH-mm-ss	
descripcion	Varchar (200)	Si	NULL	Descripción particular del respaldo	
configuracion	Varchar (1000)	Si	NULL	Script de respaldo	

SUBRED

Campo	Tipo	Nulo	Predeterminado	Comentarios	Llave
Id_subred	Int (11)	No		Identificador único de la subred	PK
lpred	Varchar (30)	Si	NULL	ip de red	
maskara	Varchar (30)	Si	NULL	maskara	
broadcast	Varchar (30)	Si	NULL	dirección ip broadcast	
estado	Int (11)	Si	NULL	1: libre se puede usar, 2 ocupada no se puede usar	
nodo	Int (11)	Si	NULL	3,4,5 según el nodo. 0 si pertenece al core	
descripción	Varchar (100)	Si	NULL	Descripción particular de la subred	

TIPO CLIENTE

Campo	Tipo	Nulo	Predeterminado	Comentarios	Llave
Id_tipo cliente	Int (11)	No		Identificador del tipo de cliente	PK
nombre	Varchar (30)	Si	NULL	Nombre	
descripción	Varchar (200)	Si	NULL	Descripción particular del tipo de cliente	



TIPOCONEXION

Campo	Tipo	Nulo	Predeterminado	Comentarios	Llave
Id_tipo conexión	Int (11)	No		Identificador único del tipo de conexión	PK
nombre	Varchar (30)	Si	NULL	nombre	
descripción	Varchar (200)	Si	NULL	Descripción particular del tipo de conexión	

TIPOEQUIPO

Campo	Tipo	Nulo	Predeterminado	Comentarios	Llave
Id_tipo equipo	Int (11)	No		Identificador único del tipo de equipo	PK
nombre	Varchar (30)	Si	NULL		
marca	Varchar (30)	Si	NULL	Marca del equipo	
modelo	Varchar (30)	Si	NULL	Modelo - serie del equipo	
descripción	Varchar (200)	Si	NULL	Descripción particular del tipo de equipo	

TIPOINTERFAZ

Campo	Tipo	Nulo	Predeterminado	Comentarios	Llave
Id_tipo interfaz	Int (11)	No		Identificador único del tipo de interfaz	PK
nombre	Varchar (30)	Si	NULL		
descripción	Varchar (200)	Si	NULL	Descripción particular del tipo de interfaz	

UBICACION

Campo	Tipo	Nulo	Predeterminado	Comentarios	Llave
Id_ubicacion	Int (11)	No		Identificador único de la	PK



				ubicación de un equipo	
sector	Varchar (200)	Si	NULL	sector donde esta ubicado el equipo	
edificio	Varchar (100)	Si	NULL	Nombre del edificio o numero de casa donde se encuentra ubicado	
latitud	Double	Si	NULL	coordenada de latitud	
longitud	Double	Si	NULL	coordenada de longitud	
descripción	Varchar (200)	Si	NULL	Descripción particular del equipo	

USUARIO

Campo	Tipo	Nulo	Predeterminado	Comentarios	Llave
id_usuario	int(11)	No		Identificador único del usuario	PK
login	varchar(30)	No		login de usuario	
clave	varchar(30)	Si	NULL	clave de usuario	
email	varchar(30)	Si	NULL	correo electrónico	
id_empleado	int(11)	Si	NULL	identificador del empleado al cual corresponde el usuario del sistema	
Id_rol	int(11)	Si	NULL	Identificador del rol del usuario	

VLAN

Campo	Tipo	Nulo	Predeterminado	Comentarios	Llave
Id_vlan	Int (11)	No		Identificador único del vlan	PK
tag	Int (11)	No		Tag o identificador del vlan	
nombre	Varchar (30)	No		Nombre de la vlan	



descripción	Varchar (100)	No		Descripción particular de la vlan	
estado	Int (11)	Si	NULL	1: activa (vlan en uso), 2: disponible (se le puede poner un ip), 3: suspendida (con ip pero deshabilitada)	

VRF

Campo	Tipo	Nulo	Predeterminado	Comentarios	Llave
Id_vrf	Int (11)	No		Identificador único del vrf	PK
Id_cliente	Int (11)	Si	NULL	Identificador del cliente para el cual fue creado el vrf	
nombre	Varchar (100)	Si	NULL	Nombre de la vrf	
rt	Varchar (50)	Si	NULL	Route target	
rd	Varchar (50)	Si	NULL	Route distinguisher	

3.3.3 Procesos de Configuración de Equipos

Antes de realizar la configuración de una red IP/MPLS hay varios temas en consideración como la ubicación estratégica de los lugares en donde estarán físicamente los LSR, planificación de la sobrecarga en la red y la distribución de los nodos involucrados en la topología de la red así como las adecuadas características de hardware con las que cada uno desempeñara su trabajo, dichos temas no son considerados en este proyecto que se enfoca en la automatización de los procesos de



configuración mas que en la arquitectura y planeación de una red IP/MPLS.

A continuación se describirán los procesos involucrados en la configuración de una red IP/MPLS

Procesos Previos de Configuración Manual

En una red que esta siendo configurada desde cero los procesos que definen el núcleo en una red IP/MPLS incluye a mas de la configuración de las direcciones ip versión 4 en el caso de la red centrosur IP/MPLS de las interfaces o puertos de red de los equipos o LSR y con especial atención la configuración de la interfaz “loopback 1” del equipo, esta interfaz lógica del equipo se utiliza en el dominio MPLS para establecer la comunicación entre los LSR del dominio, y es la base para la configuración del protocolo BGP entre los equipos de borde del dominio MPLS.

A continuación se detallan los comandos de configuración para la interfaces y el protocolo IGP que en este caso es ospf

Configuración de direccionamiento IP

```
router# config terminal
```

```
router(config)# interface “serial 0/0”
```

```
router(config-if)# ip address “ip” “mascara”
```

```
router(config-if)# no shutdown
```



```
router(config-if)# description "text descriptivo"
```

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

Configuración de IGP

```
router (config)#router ospf "process-id"
```

```
router (config-router)#network "ip-red" "wildcard-mask" area "area-id"
```

Configuración del acceso a la consola a través de telnet y creación de usuarios con privilegios de administración

```
router# config terminal
```

```
router(config)# line vty 0 4
```

```
router(config-line)# login local
```

```
router(config)# username "usuario" privilege "15" password "clave"
```

Estos datos del "usuario" y "clave" para el administrador del equipo tendrán que ser ingresados en el sistema al momento de agregar un equipo ya que dicha información se utilizara en los script del sistema donde se automatiza la configuración.

El dato donde se especifica la propiedad "privilege" con nivel 15 indica que el usuario tendrá un rol administrativo lo que le permite el acceso y ejecución de cualquier tarea de configuración dentro del equipo.



Queda a disposición del usuario los datos de administración que ingrese al momento de agregar un equipo al sistema, siendo recomendable un privilegio con nivel 15.

Los procesos de configuración anteriormente expuestos contemplan la previa configuración manual básica que el sistema requiere antes de entrar en producción en un dominio MPLS. Estos procesos no pueden automatizarse mediante scripts en la aplicación ya que en si mismos establecen el entorno que permite el acceso del sistema a los equipos.

Automatización de los Procesos de Configuración

En el caso del presente proyecto actualmente la Empresa Eléctrica Regional Centrosur Cuenta con un core MPLS en producción configurado en su totalidad y funcional, por lo en este punto el sistema deberá estar en capacidad de acceder a cualquier equipo dentro del core de la red creada para el dominio MPLS de Centrosur.

La automatización de los procesos de configuración se ejecuta en script programados en código java que utiliza la extensión ExpectJ, mediante el despliegue de pseudoterminales que interactúan con los procesos interactivos como el acceso telnet a la consola de administración de un router, en el siguiente ejemplo se describirá el funcionamiento de un script java que utiliza la extensión expectJ para automatizar procesos interactivos:

En este ejemplo se interactúa mediante un acceso de tipo telnet con un router cisco para ingresar al modo de configuración global.



```
public void telnet() throws Exception
{
    ExpectJ exp = new ExpectJ(50);
    String command = "telnet 192.168.241.160";
    Spawn sp = exp.spawn(command);
    sp.expect("Username:");
    sp.send("Admin\n");
    sp.expect("Password:");
    sp.send("mypassword\n");
    sp.expect("router#");
    sp.send("configure terminal\n");
    sp.expect("router(config)#");
    sp.send("exit\n");
    sp.stop();
    System.out.println("Cerrada la sesion telnet.");
}
```

La línea: ***ExpectJ exp = new ExpectJ(50);*** crea un objeto de tipo ExpectJ especificando un tiempo de 50 segundos como “defaultTimeoutSeconds”, dicho valor indica el periodo máximo que el proceso estará en espera de una respuesta esperada válida que cumpla con los parámetros establecidos para la interacción antes de dar por terminada la interacción.

En la línea ***String command = "telnet 192.168.241.160";*** se crea una variable de tipo string donde especifico el tipo de proceso con el cual se interactuara, en este caso telnet, y la entidad con la que se establecerá este proceso interactivo, para este caso es el equipo con la ip 192.168.241.160.

En la línea: ***Spawn sp = exp.spawn(command);*** se crea el objeto sp de tipo spawn que será el encargado de “hablar” con el proceso especificado en la variable command, es decir, es quien interactuara con el proceso, tanto de leer las entradas de respuesta como de escribir o enviar la respuesta para continuar con la interacción del proceso.



Esta línea: ***sp.expect("Username:");*** es la primera línea de interacción y se interpreta como la espera por una respuesta del proceso con el contenido "Username:", cuando el objeto sp de tipo Spawn lea una entrada similar procederá en la siguiente línea donde envía/escibe una respuesta para continuar con la interacción.

En la línea: ***sp.send("Admin\n");*** el objeto sp de tipo Spawn escribe Admin como la respuesta para continuar con la interacción, después de que realiza dicha acción nuevamente pasa al estado de espera por la respuesta de proceso.

Esta es la manera en que se interactúa con el proceso, cuando se ha concluido y se ha realizado la ejecución hasta el punto requerido se utiliza ***sp.stop();*** para dar por concluida la interacción.

A continuación se detallan los procesos más relevantes que han sido automatizados y que pueden ser configurados en los equipos desde el sistema prototipo del presente proyecto.

Nombre: SCRIPT G3

Habilita el protocolo mpls de forma global y sobre una interfaz de un equipo P o PE que se conecta a un P o PE.

Tipo Script	Script
Manual	<pre>"hostname">enable "hostname"#conf t "hostname"(config)#mpls ip "hostname"(config)#int "interface1" "hostname"(config-if)#mpls ip</pre>
Automatizado	<pre>public void scriptg3(String hn, String ip, String user, String pass, String interfaz) throws Exception</pre>



```

{
    ExpectJ exp = new ExpectJ(50);
    String command = "telnet " + ip;
    Spawn sp = exp.spawn(command);
    sp.expect("Username:");
    sp.send(user + "\n");
    if (sp.isClosed()) {
        System.err.println("Did not match");
        System.exit(1);
    }

    sp.expect("Password:");
    sp.send(pass + "\n");
    sp.expect(hn + "#");
    sp.send("configure terminal\n");
    sp.expect(hn + "(config)#");
    sp.send("mpls ip\n");
    sp.expect(hn + "(config)#");
    //ethernet 1/5
    sp.send("interface " + interfaz + "\n");
    sp.expect(hn + "(config-if)#");
    sp.send("mpls ip\n");
    sp.expect(hn + "(config-if)#");
    sp.send("exit\n");
    sp.expect(hn + "(config)#");
    sp.send("exit\n");
    sp.expect(hn + "#");
    sp.send("wr\n");
    sp.expect(hn + "#");
    sp.stop();
    System.out.println("Cerrada la sesion telnet.");
}

```

Script configurado en la clase: mpls.java del sistema:

Nombre: SCRIPT PE20:

Configuración de MP-BGP en un equipo de tipo PE

Tipo Script	Script
Manual	<pre> PE_A(config)#router bgp "sistema_autonomo" PE_A(config-router)#no bgp default ipv4-unicast PE_A(config-router)#neighbor "ip_loopback_PE_B" remote-as "sistema_autonomo" PE_A(config-router)#neighbor "ip_loopback_PE_B" update-source lo0 -1 PE_A(config-router)#address-family vpnv4 PE_A(config-router-af)#neighbor "ip_loopback_PE_B" activat </pre>
Automatico	<pre> public void scriptPE20(String hn, String ip, String user, String pass, String SA, String remotope) throws Exception { ExpectJ exp = new ExpectJ(50); String command = "telnet " + ip; Spawn sp = exp.spawn(command); sp.expect("Username:"); sp.send(user + "\n"); if (sp.isClosed()) { System.err.println("Did not match"); System.exit(1); } } </pre>



```

sp.expect("Password:");
sp.send(pass + "\n");
sp.expect(hn + "#");
sp.send("configure terminal\n");
sp.expect(hn + "(config)#");
sp.send("router bgp " + SA + "\n");
sp.expect(hn + "(config-router)#");
sp.send("no bgp default ipv4-unicast\n");
sp.expect(hn + "(config-router)#");

sp.send("neighbor " + remotope + " remote-as " + SA + "\n");
sp.expect(hn + "(config-router)#");

sp.send("neighbor " + remotope + " update-source lo 0\n");
sp.expect(hn + "(config-router)#");
sp.send("address-family vpnv4\n");
sp.expect(hn + "(config-router-af)#");
sp.send("neighbor " + remotope + " activate\n");

sp.send("exit\n");
sp.expect(hn + "(config-router)#");
sp.send("exit\n");

sp.expect(hn + "(config)#");
sp.send("exit\n");
sp.expect(hn + "#");
sp.send("wr\n");
sp.expect(hn + "#");
sp.stop();
system.out.println("Cerrada la sesion telnet.");

```

Para probar al configuración podemos utilizar el siguiente comando:

PE_B#sh ip bgp neigh "ip_loopback_PE_A"

Considerando como los equipo PE_A y PE_B a los nodos involucrados en las subredes para la subred virtual configurada en IP/MPLS.

Nombre: SCRIPTPE2:

Creación de la Vrf, esta dentro de la clase mpls.java

Tipo Script	Script
Manual	<pre> "hostname"(config)#ip vrf "name_vrf" "hostname"(config-vrf)#route-target "name_rt" "hostname"(config-vrf)#rd "name_rd" "hostname"(config-vrf)#exit </pre>
Automatizado	<pre> public void scriptPE2(String hn, String ip, String user, String pass, String namevrf, String rt, String rd) throws Exception { ExpectJ exp = new ExpectJ(50); String command = "telnet " + ip; </pre>



```

Spawn sp = exp.spawn(command);
sp.expect("Username:");
sp.send(user + "\n");

if (sp.isClosed()) {
    System.err.println("Did not match");
    System.exit(1);
}

sp.expect("Password:");
sp.send(pass + "\n");
sp.expect(hn + "#");
sp.send("configure terminal\n");
sp.expect(hn + "(config)#");
sp.send("ip vrf " + namevrf + "\n");
sp.expect(hn + "(config-vrf)#");

sp.send("route-target " + rt + "\n");

sp.expect(hn + "(config-vrf)#");
sp.send("rd " + rd + "\n");
sp.expect(hn + "(config-vrf)#");
sp.send("exit\n");
sp.expect(hn + "(config)#");
sp.send("exit\n");
sp.expect(hn + "#");
sp.send("wr\n");
sp.expect(hn + "#");
sp.stop();
System.out.println("Cerrada la sesion telnet.");
}
    
```

Nombre: SCRIPT PE3

Configuración ipv4 de interfaz PE, subred PE-CE

Tipo Script	Script
Manual	<pre> "hostname"config)#router rip "hostname"(config-router)#version 2 "hostname"(config-router)#address-family ipv4 vrf "name_vrf" "hostname"(config-router-af)#version 2 "hostname"(config-router-af)#network "ip_red" "hostname"(config-router-af)#no auto-summary redistribucion de RIP-BGP y viseversa "hostname"(config)#router bgp "sistema_autonomo" "hostname"(config-router)#address-family ipv4 vrf "name_vrf" "hostname"(config-router-af)#redistribute rip metric 1 "hostname"(config)#router rip "hostname"(config-router)#address-family ipv4 vrf "name_vrf" "hostname"(config-router-af)#redistribute bgp "sistema_autonomo" mk </pre>
Automatizado	<pre> public void scriptPE5(String hn, String ip, String user, String pass, String namevrf, String net, String SA) throws Exception { ExpectJ exp = new ExpectJ(50); String command = "telnet " + ip; </pre>



```
Spawn sp = exp.spawn(command);
sp.expect("Username:");
sp.send(user + "\n");

if (sp.isClosed()) {
    System.err.println("Did not match");
    System.exit(1);
}
sp.expect("Password:");
sp.send(pass + "\n");
sp.expect(hn + "#");
sp.send("configure terminal\n");
sp.expect(hn + "(config)#");

//Configuracion RIP para la VRF

sp.send("router rip\n");
sp.expect(hn + "(config-router)#");
sp.send("version 2\n");
sp.expect(hn + "(config-router)#");
sp.send("address-family ipv4 vrf " + namevrf +
"\n");
sp.expect(hn + "(config-router-af)#");
sp.send("version 2\n");
sp.expect(hn + "(config-router-af)#");
sp.send("network " + net + "\n");
sp.expect(hn + "(config-router-af)#");
sp.send("no auto-summary\n");
sp.expect(hn + "(config-router-af)#");
sp.send("exit\n");
sp.expect(hn + "(config-router)#");
sp.send("exit\n");
sp.expect(hn + "(config)#");
//Redistribucion de RIP-BGP y viseversa

sp.send("router bgp " + SA + "\n");
sp.expect(hn + "(config-router)#");
sp.send("address-family ipv4 vrf " + namevrf +
"\n");
sp.expect(hn + "(config-router-af)#");
sp.send("redistribute rip metric 1\n");
sp.expect(hn + "(config-router-af)#");
sp.send("router rip\n");
sp.expect(hn + "(config-router)#");
sp.send("address-family ipv4 vrf " + namevrf +
"\n");
sp.expect(hn + "(config-router-af)#");
sp.send("redistribute bgp " + SA + " metric 1\n");
sp.expect(hn + "(config-router-af)#");
sp.send("exit\n");
sp.expect(hn + "(config-router)#");
sp.send("exit\n");
sp.expect(hn + "(config)#");

//FIN REDISTRIBUCION

sp.send("exit\n");
sp.expect(hn + "#");
sp.send("wr\n");
sp.expect(hn + "#");
sp.stop();
System.out.println("Cerrada la sesion telnet.");
}
```

Configuración de los Customer Edge o CE



La configuración de los equipos de acceso o CE tiene q ser realizada manualmente, para dicho trabajo se debe utilizar la siguiente configuración:

```
# interface e1/0
# ip address 10.1.1.2 255.255.255.252
# no sh
# router rip
# version 2
# network 10.0.0.0
# no auto-summa
# conf t
```

Automatización del proceso de respaldos

Con el siguiente script se automatiza el proceso de guardar la configuración de un equipo router cualquiera al que el sistema tenga acceso y pueda conectarse:

```
public void scriptRespaldo(String hn, String ip, String user, String pass, String fecha) throws
Exception
{
//creamos el archivo en el tftp con la fecha actual

    ExpectJ exp2 = new ExpectJ(50);
    String command2 = "telnet 127.0.0.1";
    Spawn sp2 = exp2.spawn(command2);
    sp2.expect("login:");
    sp2.send(user + "\n");
    if (sp2.isClosed()) {
        System.err.println("Did not match");
        System.exit(1);
    }

    sp2.expect("Password:");
    sp2.send("paul010\n");
    sp2.expect("paul@ubuntu:~$");
    sp2.send("cd /var/lib/tftpboot\n");
    sp2.expect("paul@ubuntu:/var/lib/tftpboot$");
    sp2.send("touch " + hn + "-config-" + fecha + "\n");
    sp2.expect("paul@ubuntu:/var/lib/tftpboot$");
    sp2.send("chmod 777 " + hn + "-config-" + fecha + "\n");
    sp2.expect("paul@ubuntu:/var/lib/tftpboot$");
    sp2.stop();
    System.out.println("Cerrada la sesion telnet para rftp.");

//subimos el respaldo al tftp
    ExpectJ exp = new ExpectJ(50);
    String command = "telnet " + ip;
    Spawn sp = exp.spawn(command);
    sp.expect("Username:");
```



```
sp.send(user + "\n");
if (sp.isClosed()) {
    System.err.println("Did not match");
    System.exit(1);
}

sp.expect("Password:");
sp.send(pass + "\n");

sp.expect(hn + "#");
sp.send("copy run tftp\n");
sp.send("192.168.241.170\n");
sp.send(hn + "-config-" + fecha + "\n");

sp.expect(hn + "#");
sp.send("wr\n");
sp.expect(hn + "#");

sp.stop();
System.out.println("Cerrada la sesion telnet.");

}
```

El script trabaja mutuamente con un servidor tftp donde se almacenan los script de respaldo de los equipos, el sistema crea un archivo dentro del servidor tftp y sobre el cual se escribe la configuración del equipo.

3.3.4 Procesos de Monitoreo de Equipos

Para el presente proyecto se contempla el uso de snmp en su versión v2c para el monitoreo de sucesos en los equipos. El modulo de monitoreo se implemento a partir de la API de webNMS, se programo la clase trapreceiver para capturar los paquetes tipo trap enviados por los agentes snmp de los equipos de red, asi como una clase SNMPGet donde se puede configurar la solicitud especifica de información que se solicita, a continuación se detalla el código de la clase SNMPGet:

```
package com.snmp;
import com.adventnet.snmp.snmp2.*;

public class SnmpGet {

    public String getUptime(String ip) {
```



```
//Inicializamos el SNMP target bean
SnmpAPI api = new SnmpAPI();
SnmpSession session = new SnmpSession(api);
try {
    session.open();
    //Contruimos nuestra GET Request PDU

    SnmpPDU pdu = new SnmpPDU();
    UDPProtocolOptions option = new UDPProtocolOptions(ip);
    pdu.setProtocolOptions(option); //sets the host in which the agent is running
    pdu.setCommand(SnmpAPI.GET_REQ_MSG);
    //Especificamos el OID Requerido
    SnmpOID oid = new SnmpOID(".1.3.6.1.2.1.1.3.0"); //Here the OID is .1.3.6.1.2.1.1.0

    pdu.addNull(oid);
    SnmpPDU result;

    result = session.syncSend(pdu);
    session.close();
    api.close();
    //Retornamos la variable capturada
    return " Uptime: " + result.getVariable(0).toString();

} catch (SnmpException e) {
    // TODO Auto-generated catch block
    return e.toString();
}
}
```

La configuración mínima recomendada para los equipos de la red a fin de que emitan mensajes snmp de tipo trap es la siguiente:

```
Router# conf t
Router(config)# snmp-server community public RW
Router(config)# snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
Router(config)# snmp-server host 192.168.241.170 inform version 2c public snmp
Router(config)# end
```

La propiedad “community” en la línea dos, especifica el nombre de la comunidad que intercambiara mensajes snmp y al decir “RW”, estamos diciendo que el Manager puede tanto leer como escribir en los MIBs del equipo, permitiendo así la configuración y el monitoreo a través de snmp. En la línea 3 con la propiedad “enable” podemos especificar el tipo de mensajes que se emitirán con snmp como lo es el caso de traps que son



mensajes no solicitados emitidos por los agentes, así también se pueden indicar mediante la sentencia enable eventos específicos como linkup o linkdown por ejemplo que le indican al Manager que un puerto del equipo se levanto (linkup) o se cayo el enlace en el caso de linkdown.

En la cuarta línea la propiedad "host" específica la dirección ip del manager a donde serán enviados los mensajes snmp, la dirección ip puede ser remplazada por el FQDN del servidor manger snmp en caso de contar con esquema donde se utilicen nombres de dominio. En esta sentencia se especifica también la versión del protocolo a utilizar y el nombre de la comunidad para el envío de mensajes.

Esta configuración al momento esta presente en los equipos de la red MPLS de Centrosur por lo que no representa cambios ni modificaciones adicionales.

3.3.5 Interfaz

La capa de interfaz se desarrollo en Action Script en su versión 3, donde ya se puede utilizar el modelo orientado a objetos, con componentes mxml (Macromedia eXtensible Markup Language) desarrollado en el 2005 por Macromedia y que actualmente forma parte del sdk Flex de Adobe. A continuación se presenta la estructura del componente más el código action script.

```
<?xml version="1.0" encoding="utf-8"?>

<mx:VBox xmlns:mx="http://www.adobe.com/2006/mxml"
width="100%" backgroundColor="#FFFFFF" borderStyle="solid" horizontalAlign="center"
verticalAlign="middle"
creationComplete="getClientes()"
height="100%"
xmlns:dataGrid="com.view.*">
```



```
<mx:Script>
<![CDATA[
import mx.controls.Alert;
import mx.collections.*;
import com.vo.cliente.*;

[Bindable]private var clientes: ArrayCollection = new ArrayCollection();

private function getClientes():void
{
    SrvLCliente.getClientes();
}

public function r_SrvLCliente(e:Object):void
{
    this.modelcliente.clientes=e.result as ArrayCollection;
}

public function e_SrvLCliente(e:Object):void
{
    var faultEvent : FaultEvent = FaultEvent( e );
    Alert.show("error, respuesta server: " + e.message.toString());
}

]]>
</mx:Script>

<mx:DataGrid id="myGrid" dropShadowEnabled="true" rowCount="5" width="100%"
rowHeight="40" dataProvider="{this.clientes}" itemClick="itemClickEvent(event);">

    <mx:columns>
        <mx:DataGridColumn dataField="nombre" />
        <mx:DataGridColumn dataField="telefono"/>
    </mx:columns>

</mx:DataGrid>

</mx:HBox>

<mx:RemoteObject id="SrvLCliente" destination="clienteService" result="r_SrvLCliente(event)"
fault="e_SrvLCliente(event)" showBusyCursor="true"/>

<mx:Binding source="{this.modelcliente.clientes}" destination="setClientes"/>

</mx:VBox>
```

En el ejemplo expuesto se configuro un objeto tipo *RemoteObject* llamado *SrvLCliente* que se comunicara con el Servicio *getClientes* Implementado en la clase java *clienteService* del lado del servidor que se comunica con la base de datos para obtener el listado de clientes. A partir de esto la variable local denominada *clientes* se alimenta del



resultado obtenido por el Remote Objet, y a su vez se convierte en el proveedor de datos de el control tipo *DataGrid* denominado *myGrid*.

Todo este proceso inicia con la propiedad *creationComplete="getClientes()",* declarada inicialmente en el script. Esta estructura se utilizo para la elaboración de toda la interfaz de usuario.

3.3.6 Ambiente de Producción

EL ambiente de producción del sistema es netamente Web, ya que esta elaborado como base en la plataforma Java se utilizar el entorno de aplicaciones Apache Tomcat que presenta las condiciones ideales para la ejecución del sistema.

Para el sistema operativo se ha escogido como GNU/Linux por presentar estabilidad, y seguridad en comparación con las opciones del mercado, en tal caso se ha escogido la distribución CentOS derivada de Red Hat.

Dada la falta de disposición de un Servidor Dedicado para este fin se ha dispuesto la Virtualización del hardware para la creación de servidores virtuales con las características requeridas para el sistema

3.3.7 Entorno Virtual



Universidad de Cuenca

En esta etapa se describirá la implementación de Virtualización que se llevo a cabo, para a su vez tener la disponibilidad de un servidor donde alojar la aplicación.

Para la implementación de un Entorno Virtual se realizo el análisis del tipo de hardware disponible en el Data Center de la Dirección de Telecomunicaciones de la Empresa Eléctrica Regional Centro Sur en cuento a Servidores y Almacenamiento.

Servidores

Los equipos blade HP bladesystem G5 del centro de datos, poseen la tecnología IntelVT en sus procesadores Xeon que les permiten soportar el modelo de trabajo para Virtualización en Paralelo.

Storage

El data center posee un espacio de almacenamiento de tipo SAN Storage Area Network basado en la solución HP EVA que incluye un arreglo de discos con RAID a nivel de hardware con controladoras de discos físicas y una conexión de fibra mediante el protocolo FCP con los servidores del Rack, esto a través de un Switch fibra: HP STORAGE WORKS 8/8 SAN

Modelo de Virtualización

Específicamente se piensa virtualizar el equipo HP blade ubicado en la bay 4 del Rack 2, donde actualmente esta corriendo un servidor



Windows 2003 Server con apache Tomcat donde esta alojada la pagina web de CentroNet.

Se ha seleccionado la línea de Xen como tecnología de Virtualización para el datacenter de la DiTel, esta tecnología de Virtualización en paralelo cuenta con la ventaja de tener versiones de software libre con las características suficientes y necesarias para emprender una implementación como la requerida.

En base al análisis del hardware a disposición así como las herramientas de software se determino el siguiente modelo de Virtualización

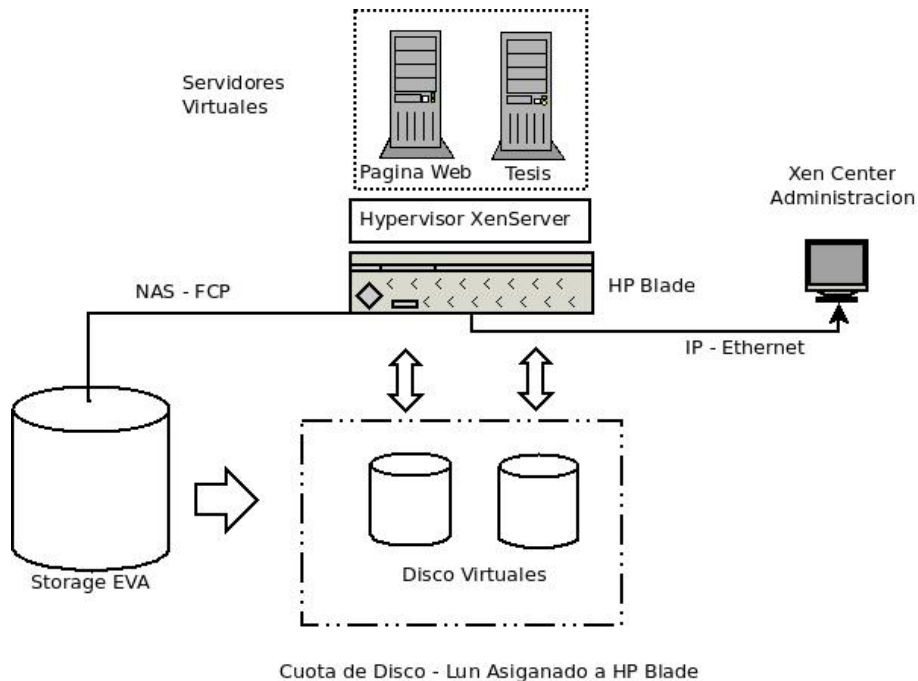


Figura 3.5 Entono Virtual

En el blade se instalo Xen Server como hypervisor, el cual esta conectado al Storage EVA HP mediante enlaces de fibra con el uso del protocolo FCP para establecer la comunicación, desde el CommandView



se presento una cuota de disco al blade donde esta instalado el hypervisor XenServer. La administración del Entorno Virtual se realiza mediante el Manager XenCenter instalado en una terminal cliente con sistema operativo Windows que puede conectarse al Hypervisor a través de la red LAN interna del DataCenter, desde ahí se gestionan los recursos físicos que posee el hypervisor, con lo que se crean discos virtuales para las maquinas virtuales que se ocuparan en la tarea de servidores de aplicaciones Java.

En cada Servidor se configurara un interfaz virtual en modo bridge a la interfaz física del servidor blade HP a modo de ubicar las maquinas virtuales en la misma Subred el hypervisor

A continuación se detallan las características del Servidor Virtual utilizado para el sistema NMS de la red Centrosur IP/MPLS.

Procesador	Memoria RAM	Disco Duro	Interfaz de Red
Intel Xeon 2,6 GHZ	3GB	30GB	eth0 (modo bridge)

A continuación de detallan los datos de Direccionamiento IP del entorno Virtual, el equipo blade físico como las maquinas virtuales tienes ip privadas en la subred 192,.168.27.0 donde se realiza NAT a ip publicas de la subred 190.120.76.0 para permitir la configuración de dominios y el acceso desde internet.



Servidor	Direccionamiento Privado		Ip Publica
	Dirección IP	Gateway	
Hypervis or XenServ er	192.168.27.62 /255.255.255.192(26)	192.168.27 .1	
TesisWe b	192.168. 27.60	192.168.27 .1	190.120.76.1 33
Centrone t Web	192.168.27.61	192.168.27 .1	190.120.76.1 32
Host Gestion	192.168.27.59 192.168.27.58	192.168.27 .1	

Se configuro el subdominio <http://nms.centronet.net.ec> para acceso a la aplicación prototipo NMS.

3.4 PRUEBAS

3.4.1 Pruebas

Pruebas del modulo de configuración

Los resultados de las pruebas del prototipo del sistema que se muestran a continuación fueron capturas realizadas de los mensajes java de que se visualizan en consola con el archivo de logs catalina.out con la ayuda de un



terminal conectados al servidor donde esta corriendo el servidor de aplicaciones Tomcat, se ejecuto el siguiente comando:

```
tail -f catalina.out
```

Dentro del directorio:

```
/usr/local/tomcat6/apache-tomcat-6.0.29/logs
```

Datos de prueba:

Para realizar la prueba se utilizaron los siguientes datos ficticios:

Datos de VRF:

Vrf: vrfest

VRF Cliente **VRF CS**

nombre: * testvrf

Tipo: * **Internet Corporativo** ▼

route distinguisher: * 28025:1522222

route-target both: * 28025:1522222

CS: * **CSIC** ▼

route-target IMPORT: * 28025:1115000002

route-target EXPORT: * 28025:1115000001

Datos de Cliente:

nombre	telefono	plan	Estado	deuda	Tipo	# Contrato
cliente A			Activo		corporativo	11111
cliente B			Activo		residencial	22222

Nombre: Cliente A

#contrato: 22222



Universidad de Cuenca

Estado: activo

Equipo de Prueba:

hostname: PE_SE3

puerto fisico: G1/4

Subred 190.120.67.4

Capturas de pantalla de pruebas:

Configuración de Vrf

```
root@ubuntu: /usr/local/tomcat6/apache-tomcat-6.0.26/webapps
File Edit View Terminal Tabs Help
root@ubuntu: ~ root@ubuntu: /usr/... root@nms: /usr/loc... root@ubuntu: /usr/l...
User Access Verification
Username: automatico
Password:
PE_SE3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
PE_SE3(config)#ip vrf testvrf
PE_SE3(config-vrf)#rd 28025:1522222
PE_SE3(config-vrf)#export map RM-NMS
PE_SE3(config-vrf)#route-target import 28025:1522222
PE_SE3(config-vrf)#route-target export 28025:1522222
PE_SE3(config-vrf)#route-target import 28025:1115000002
PE_SE3(config-vrf)#route-target export 28025:1115000001
PE_SE3(config-vrf)#route-target import 28025:50000000
PE_SE3(config-vrf)#exit
PE_SE3(config)#exit
PE_SE3#wr
Building configuration...
[OK]
PE_SE3#Cerrada la sesion telnet.
Inicio insertar relacion vrfequipo, crud
Fin save relacion vrfequipo, crud
Listado Completo vrfs
```

Figura 3.6 Configuración Vrf

Configuración de un puerto físico



Router: * PE_SE3

Modo: * Port
 Vlan
 Port-vlan

Ports: * e1/5

Tag Vlan: * Vlan.

Descripcion: * cliente A

Vrf: * testvrf

Subred: * 190.120.67.4

Figura 3.7 Parámetros Puerto Físico

Resultados de la configuración:



```
root@ubuntu: /usr/local/tomcat6/apache-tomcat-6.0.26/webapps
File Edit View Terminal Tabs Help
root@ubuntu: ~ x root@ubuntu: /usr/... x root@nms: /usr/loc... x root@ubuntu: /usr/l... x
Connected to 50.100.0.2.
Escape character is '^]'.

User Access Verification

Username: automatico
Password:
PE_SE3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
PE_SE3(config)#interface e1/5
PE_SE3(config-if)#ip vrf forwarding testvrf
% VRF testvrf not configured.
PE_SE3(config-if)#description mydescription
PE_SE3(config-if)#ip address 190.120.67.6 255.255.255.252
PE_SE3(config-if)#no sh
PE_SE3(config-if)#exit
PE_SE3(config)#exit
PE_SE3#wr
Building configuration...
[OK]
PE_SE3#Cerrada la sesion telnet.
Inicio actualizar estado de la ip
Fin actualizar estado de la ip
```

Figura 3.8 Configuración Puerto Físico

De esta manera se realizaron las pruebas de todos los scripts que automatizan las configuraciones obteniendo resultados satisfactorios en cada prueba

Resultados de la pruebas de respaldo de equipos:



```
root@ubuntu: /usr/local/tomcat6/apache-tomcat-6.0.26/webapps
File Edit View Terminal Tabs Help
root@ubuntu... x root@ubuntu... x root@nms:/... x root@ubuntu... x root@ubuntu...
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

No directory, logging in with HOME=/
$ cd /var/lib/tftpboot
$ touch PE_SE3-config-2011-06-08-12-59-52
$ chmod 777 PE_SE3-config-2011-06-08-12-59-52
$ Cerrada la sesion telnet para rftp.
Trying 50.100.0.2...
Connected to 50.100.0.2.
Escape character is '^]'.

User Access Verification

Username: automatico
Password:
PE_SE3#copy run tftp
Address or name of remote host []? 190.120.76.133
Destination filename [pe_se3-config]? PE_SE3-config-2011-06-08-12-59-52

PE_SE3#wr
Building configuration...
[OK]
PE_SE3#Cerrada la sesion telnet.
Base Conectada
Inicio insertar respaldo
Fin save Item, respaldo equipo
Equipo respaldado
```

Figura 3.9 Respaldo de Configuración

Pruebas de Monitoreo

Las pruebas de monitoreo se realizaron en el mismo sistema constatando los datos capturados por el sistema con información del equipo, a continuación una imagen con el resultado del monitoreo realizado al equipo.



Listado General de Equipos

Hostname	Descripcion	Jerarquia
PE_SE3	PE_SE3	Provider Edge - PE

IP: 50.100.0.2	Uptime: 0 hours, 21 minutes, 1 seconds	IOS Version: CW_VERSION\$12.4(4)T1\$	Free Memory: 139141608
IP: 50.100.0.2	Uptime: 0 hours, 20 minutes, 56 seconds	IOS Version: CW_VERSION\$12.4(4)T1\$	Free Memory: 139141608
IP: 50.100.0.2	Uptime: 0 hours, 20 minutes, 53 seconds	IOS Version: CW_VERSION\$12.4(4)T1\$	Free Memory: 139141608
IP: 50.100.0.2	Uptime: 0 hours, 20 minutes, 46 seconds	IOS Version: CW_VERSION\$12.4(4)T1\$	Free Memory: 139141608
IP: 50.100.0.2	Uptime: 0 hours, 20 minutes, 42 seconds	IOS Version: CW_VERSION\$12.4(4)T1\$	Free Memory: 139141608

Figura 3.10 Monitoreo



CAPITULO IV

CONCLUSIONES Y

RECOMENDACIONES



4 CAPITULO IV: CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

Del trabajo de implementación del prototipo del sistema NMS para una red IP/MPLS se concluye lo siguiente:

De la Investigación

Una vez realizada la investigación se concluye que en el mercado hay muy pocas opciones de NMS que trabajen en la Gestión de Configuraciones, una de las áreas del modelo FCAPS, mientras que para el monitoreo existe una gran cantidad de sistemas tanto comerciales como de software libre, de esto la concluye que es muy difícil elaborar un sistema donde se pueda generalizar las necesidades en cuanto a gestión de la configuración que posee cada red de comunicación en particular.

Existen varias alternativas en cuanto a herramientas dentro del software libre para el desarrollo de aplicaciones que automaticen procesos de configuración en equipos con terminales de administración mediante consola

Se están tomado especial énfasis en la implementación de medidas de seguridad en todo lo referente a protocolos de red, esto se refleja claramente con la versión *snmpv3* donde se incluyen procesos de encriptación y otros.

Del desarrollo del prototipo



Una vez efectuada las etapas de requerimientos y análisis se observa que la gestión de los datos generados a partir de las configuraciones realizadas en redes de grandes proporciones no se administra de una manera correcta, ya que en la mayoría de los casos simplemente se editan documentos de Excel que no son centralizados, sin un control de edición de la información mas que el que pueda darle los mismo operadores de la red al documento.

Así también la gestión de configuración al desarrollarse manualmente conlleva perdida de tiempo en procesos que son repetitivos y tediosos.

La plataforma java es muy flexible y cuenta con varias extensiones que proporcionan características adicionales a las aplicaciones que se desarrollan basadas en este modelo. En el caso del prototipo fue posible la integración de Librerías que proporcionan características funcionalidades como webNMS o ExpectJ, combinado con el desarrollo de aplicaciones ricas de internet.

Un NMS que proporcione gestión de las configuraciones y que se encuentre adaptado a las necesidades de un red de datos en producción, facilita su administración, mejorando los tiempos de configuración, evitando la ejecución de errores y presentando al operador información obtenida a partir de los datos generados en las tareas de configuración.



La Virtualización es un método que permite aprovechar al máximo los recursos de hardware que se disponen, aportando ahorros tanto económicos como logísticos para cualquier institución que este en la posibilidad de implementar un entorno de Virtualización con su hardware existente.

La mayor parte de inconvenientes que se presentaron en este proyecto fue la integración de herramientas de desarrollo en un entorno de software libre ya que la documentación oficial en muchos casos no se encuentra a disposición.

El modelo RUP propuesto inicialmente para el desarrollo del sistema no resulta de gran utilidad cuando se trabaja de manera individual en el desarrollo del proyecto y el modelo UML por si solo satisfizo las necesidades para el desarrollo del proyecto

4.2 RECOMENDACIONES

Durante el proceso de implementación de proyecto el editor de la herramienta utilizada para programar la interfaz (Flex SDK) fue descontinuado por parte la empresa propietaria para el desarrollo en ambientes de software libre como lo es el sistema Operativo GNU/Linux, por lo que se recomienda realizar un análisis para comparar la factibilidad de adquirir la herramienta legacy o cambiar el software utilizado para la capa de interfaz. A pesar de esto el SDK como tal aun se puede utilizar para la programación



en ambientes de desarrollo de software libre pero sin las ventajas de un editor grafico y con un compilador basado en comandos.

Realizar una adopción del sistema de manera progresiva, cumpliendo etapas. Migración de la información actualmente disponible, elaboración de un plan de restauración de errores en caso de fallo del sistema, Capacitación del personal que brindara mantenimiento al sistema, capacitación del personal que manejara el sistema y adopción paulatina de las herramientas que posee el sistema.

Se recomienda realizar un análisis de factibilidad costo beneficio para emprender un proyecto de Virtualización del datacenter con herramientas corporativas como Red Hat Enterprise Virtualization, que proporcionan varias características en cuanto a desempeño y mantenimiento de un Centro de Datos permitiendo implementar alta disponibilidad, migración en caliente, redistribución de carga, a mas de implementar el modelo de Full virtualization donde el hypervisor trabaja a nivel del Kernel del sistema operativo.

4.3 TRABAJOS FUTUROS

Un trabajo futuro que se piensa realizar es la implementación de un modulo adicional de escaneo de redes basado en snmp que evite el proceso manual del ingreso de los nodos en la aplicación, dejando para el usuarios el ingreso de datos externos al hardware del equipo como ubicación, y otros.



A futuro se tiene pensando utilizar el API WebNMS low level junto con componentes de UI para la elaboración de módulos que implementen seguridad con el uso de snmp v3 para el manejo de dispositivos.

Se tiene pensado la implementación de un modulo para el calculo de coberturas en zonas inalámbricas, con la ayuda de Google Earth en su versión para Java Script que puede ser integrado al sistema NMS del presente proyecto. Tomando en cuenta el inconveniente presente en el API de Google Earth disponible actualmente solo para Windows y para Mac OS X 10.4 o versiones posteriores. Se esta considerando alternativas a google maps para el proyecto.

Implementación de un modulo de estadísticas con la información almacenada en la base de datos producto de monitoreo a los equipos a través del protocolo snmp. Con el uso de formas graficas como charts, pay, etc. aprovechando las ventajas que ofrece la interfaz en Action Script con flashplayer que posee el sistema.

Publicar un modulo de configuraciones estándar como proyecto hospedado en Google Project.

4.4 GLOSARIO

- EMS



Element Management System, son sistemas o aplicaciones relacionadas con el manejo de elementos de red, donde se gestionan las funciones y capacidades de cada element de red, mas no la gestion de trafico entre los elementos de Red

- **NMS**

(Network Management System) sistemas o aplicaciones que realizan la gestión de redes de datos, monitoreo del estado de los elementos y tareas de administración en la red.

- **Ajax**

Técnica de desarrollo web para crear aplicaciones interactivas

- **Atom**

Conexión de datos a nivel de capa 2 que forma parte del protocolo ip- mpls

- **Clear canal**

Es un enlace entre de dos o mas puntos cuyo configuración de direccionamiento de capa 3 a través de internet resulta transparente para los puntos conectados viendo al enlace como una cable lógico

- **Diffserv**

Terminología para referirse a servicios diferenciados **que es un** tecnología de transmisión de datos que se basa en la asignación y restricción de recursos de red para obtener calidad de servicio

- **Expect**

Extensión de TCL scripting lenguaje que automatiza procesos con herramientas de interacción como telnet

- **FCAPS**



Modelo de gestión de redes que establece los módulos de administración con los que debe disponer un red

- **FIB**

Base de datos que establece la estructura mediante la cual se organiza la información contenida en los MIBs de los dispositivos de red

- **Intserv**

Terminología utilizada para referirse a Servicios Integrados, tecnología que integra los componentes que conforman una red de transmisión de datos a fin de proporcionar calidad de servicio.

- **Ip-mspl**

Protocolo de red que ofrece calidad de servicio mediante el establecimiento de políticas IntServ, trabaja en la capa 2 y 3 del modelo OSI

- **LSR**

Equipos de red que cumplen la función de encaminadores dentro de un dominio MPLS

- **LSP**

Camino de comunicación en un dominio MPLS que se establece por medio de la colaboración de LSRs

- **MiB**

Es una colección de definiciones que brindan información de las propiedades de un dispositivo que se pueden gestionar mediante SNMP

- **Oid**



- **Object Identifier**, es el identificador de un objeto dentro de una base de información MIB
- **Qos**
Quality of Service, Termino utilizado para referirse a la calidad de servicio en redes de comunicación.
- **RIA**
Rich internet application, definición que se utiliza para denominar una aplicación que cuenta con funciones típicas de aplicaciones de escritorio.
- **SMI**
SMI describe el modelo de información de un objeto que será incluido en la MIB de un equipo
- **SNMP**
Protocolo de networking utilizado para la gestión de equipos de red
- **TCL**
Es un lenguaje programación de script interpretado
- **TIB**
Es una tabla de información de etiquetas, utilizada por cada router dentro del dominio MPLS para el intercambio de paquetes mediante etiquetas.
- **VPLS**
VPN de capa 2 implementada en dominios IP/MPLS
- **VRF**
Es una instancia de una tabla de enrutamiento que puede ejecutarse sobre uno o varios router, de tipo Provider Edge en un dominio MPLS,



junto con otras VRFs al mismo tiempo. Cada VRF implementa una VPN de capa 3, también conocida como L3VPN.

- **FQDN**

Fully Qualified Domain Name es un denominación para un equipo en particular dentro de una red de datos que incluye el nombre del equipo o hostname y el nombre de dominio asociado a ese equipo.

- **OSPF**

Protocolo de enrutamiento de estado de enlace, utilizado como IGP en redes IP/MPLS.

4.5 ANEXOS

Manual de Usuario

Introducción

El siguiente manual del sistema NMS para gestión de configuración de una red IP/MPLS sigue paso a paso en la ejecución de las diferentes tareas que el sistema puede realizar en sus diferentes módulos.

Acceso al Sistema

El sistema fue desarrollado en una plataforma web y se encuentra hospedado en un servidor Web publicado en Internet con la siguiente dirección de dominio:

<http://nms.centronet.net.ec>

El usuario del sistema deberá especificar dicho dominio en la dirección url de cualquier navegador de internet que tenga soporte de flashplayer con versión 10 o mas y la aplicación empezara con el proceso de carga.

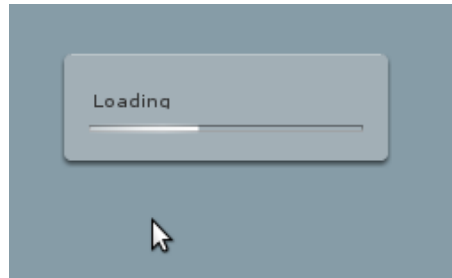


Fig A1: Carga del Sistema

Login al sistema

Una vez la aplicación se haya cargado aparecerá el cuadro para ingresar los datos de login que consiste en el clásico, nombre de usuario y contraseña, como vemos en la figura a continuación.

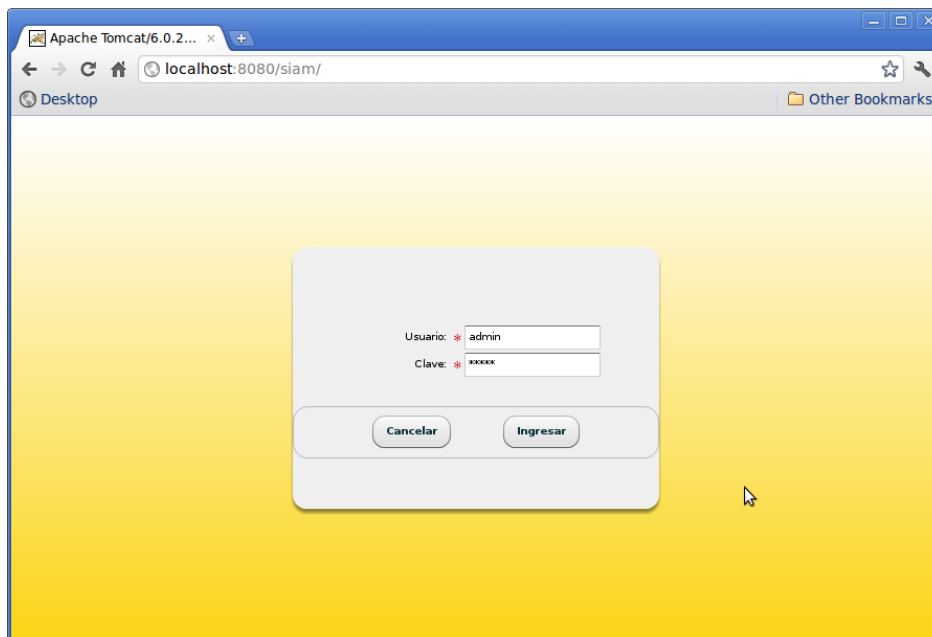


Fig A2: Vista Inicial de Login

Una vez introducida la información válida en los respectivos campos, el usuario podrá acceder al sistema dando clic en el botón "Ingresar"

Entorno de Interfaz de Usuario



La interfaz de usuario esta dividida en diferentes secciones a modo de facilitar al usuario el acceso y hacer más intuitivo el uso de sus diferentes opciones, la interfaz de usuario posee cuatro secciones principales:

- **Banner**

El banner se encuentra presente durante toda la ejecución del sistema y presenta información de la fecha y hora actual así como información de usuario que ha ingresado al sistema.

- **Menú principal**

Este menú constan los módulos de los cuales dispone el sistema:

Network.- Es esta opción se encuentra un mapa de la red MPLS así como las opciones para la gestión de configuración

Equipos.- En esta sección podemos realizar la gestión de los equipos del sistema, ingreso de nuevos equipos y sus respectivos mantenimientos, así como un listo de los respaldos de configuración de los equipos.

Utilities.- Esta opción cuenta con las herramientas de apoyo para los operadores de la red

Vlsm IPv4.-Es aquí donde se realiza la gestión de las direcciones ip versión 4 del sistema ocupadas en las configuraciones mpls de la red

clientes.- A modo de información esta sección cuenta con la base de datos de los clientes

Usuarios.- modulo que gestiona la información de los usuarios del sistema

Monitoreo.- Esta sección se encarga del monitoreo de los equipos mediante el protocolo SNMP. En la figura 3 observamos las Secciones.

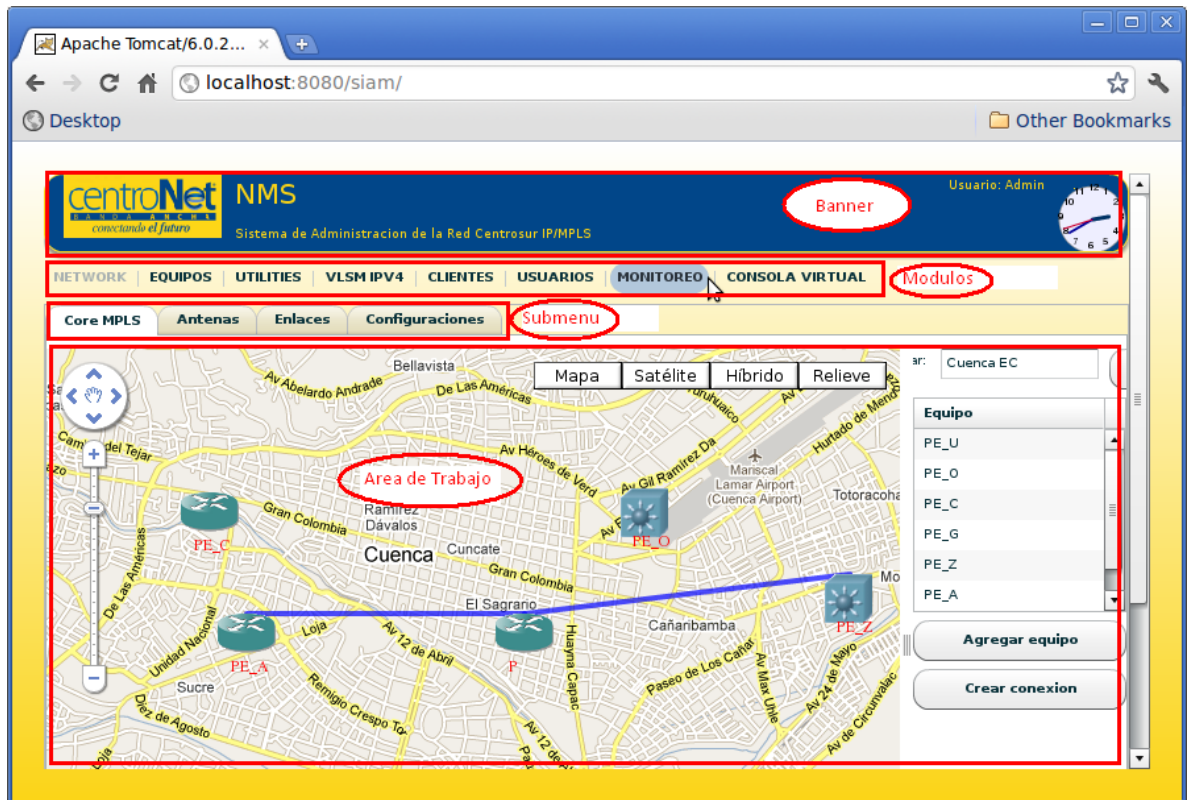


Fig A3: Secciones principales del sistema.

- **Submenú secundario**

El menú secundario dependiendo del modulo que seleccionemos despliega diferentes opciones. En la figura A3 observamos la ubicación de las opciones en cada modulo que se detallaran mas adelante

- **Área de Trabajo**

El área de trabajo depende del modulo que se seleccione, es así que en el modulo de Configuraciones con el Tab etiquetado como "Network" se tiene un googlemaps donde se grafica la topología física de le red MPLS, mientras que en el área de trabajo del modulo de usuarios se dispone de una Grilla para la gestión de los mismos, a continuación se



describirá cada una de estas áreas de trabajo con sus respectivas funcionalidades

A continuación se listan los módulos del Sistema.

1. Modulo de Configuraciones

1.1. Tab Core MPLS

Este submenú cuenta con un googlemaps con la topología de la red Centrosur IP/MPLS.

El mapa cuenta con un control de zoom que puede también gestionarse con el scroll del mouse, tiene un control de estado que informa la posición con latitud y longitud en el mapa así como el nivel de zoom actual de mapa. El mapa también tiene el control de tipo donde podemos seleccionar la vista del mapa que sea necesaria. En la figura A4 podemos ver la ubicación de los controles



Fig A4: Controles del Mapa Google Maps



Simbología del mapa:

Router



Fig A5: Imagen Icono de Router

Switch



Fig A6: Imagen Icono de Swicth

Conexión Ethernet



Conexión Fibra



Burbuja informativa

Cada icono que representa un equipo en el mapa posee una burbuja cuando se da doble clic sobre el icono que posee información del equipo, dependiendo de la Jerarquía del equipo se despliegan diferentes Tabs en la burbuja. Tabs de la burbuja:



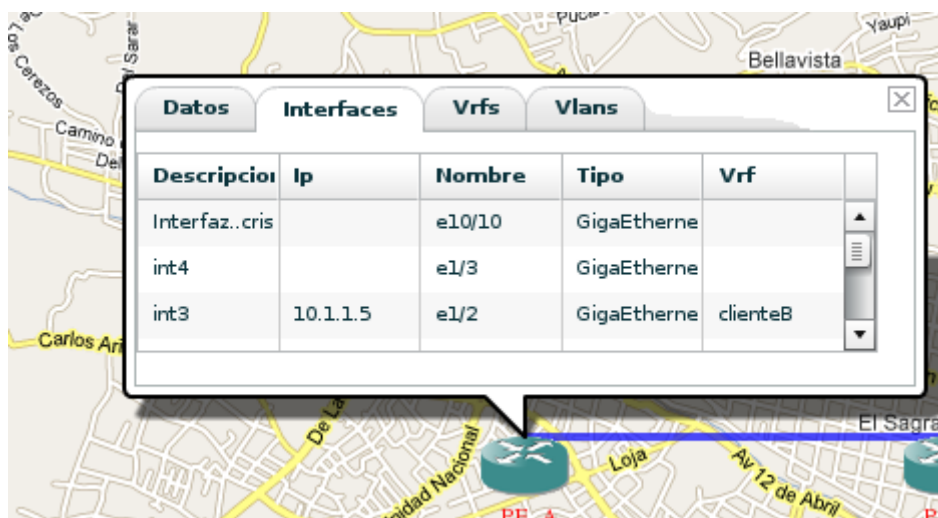
Datos.- brinda información general del equipo; nombre del equipo o hostname, jerarquía, datos del tipo de equipo y datos de la ubicación del equipo

Interfaces.- posee información de la interfaces que posee el equipo; nombre de la interfaz y en el caso de haber sido configurada, información de ip versión 4 y vrfs configuradas en la interfaz

vrf.- este Tab es valido solo para equipos de jerarquía PE y muestra un listado de las vrf configuradas en el equipo.

vlan.- este Tab es valido solo para equipos de jerarquía PE y muestra un listado de las vlans configuradas en el equipo.

Las pestañas anteriormente mencionadas se pueden ver en la figura A7



Fg A7: Burbuja Informativa

Adicionalmente en el área de trabajo de "networks" se tiene un panel donde existe un control de búsqueda para sitios georeferenciados en google maps



como nombre de ciudades, pudiendo usar filtros por país, como por ejemplo: Quito EC, en este caso el mapa automáticamente se sitúa sobre la zona geográfica y coloca un icono para indicar la ubicación. En la figura A8 observamos un ejemplo de búsqueda.



Fig A8: Controles Google Maps Usuario

En la parte inferior del control de búsqueda se encuentra un listado de los equipos presentes en el mapa, cuando hacemos un clic sobre algún equipo en el mapa se refleja esta acción abriendo la burbuja informativa del equipo, bajo este listado se encuentran 2 botones, en el equipo

Botón: "Agregar Equipo"

Este botón despliega una ventana donde se puede ingresar equipos al sistema y por ende son graficados en el mapa de google donde esta la



topología de red. Mas adelante se vera con detalle la funcionalidad de agregar equipos

Botón: "Crear Conexión"

Este botón se utiliza para activar la funcionalidad de crear una conexión física para dos equipos del mapa. Una vez activada la funcionalidad dando clic en el botón "Crear Conexión" se procede a dar un clic sobre el par de equipos involucrados sin un orden específico, una vez que hayamos dado clic en el segundo equipo dentro del mapa se despliega una ventana con las interfaces o puertos físicos de lo equipos que se seleccionaron como vemos en la siguiente figura A9

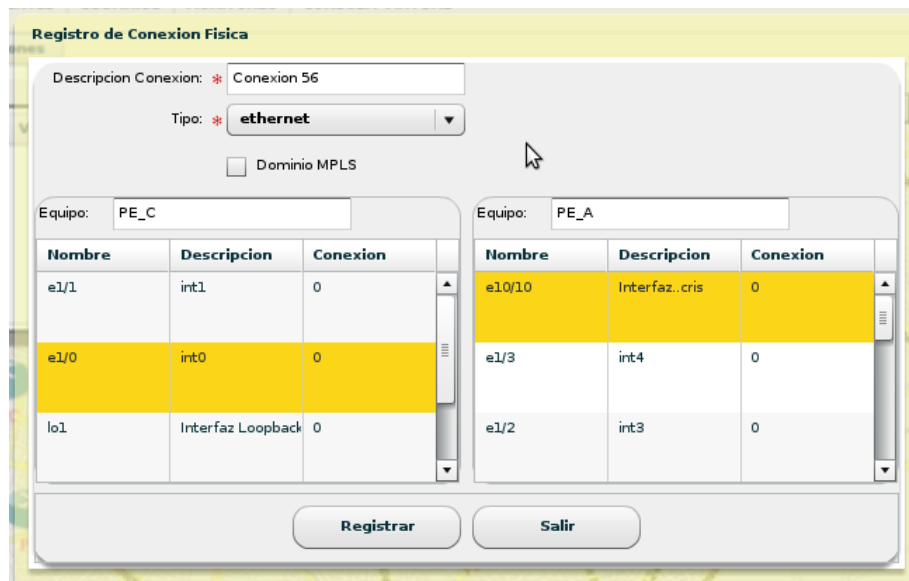


Fig A9: Vista – Ingreso de Conexión

- En el campo "Descripción Conexión" ingresamos una descripción para la conexión
- En el combo "Tipo" seleccionamos si la conexión es de tipo Ethernet o fibra óptica



- El checkbox "Dominio MPLS" indica que la conexión física esta dentro del dominio mpls
- El usuario también debe seleccionar las interfaces respectivas de los equipos que se utilizaran para la conexión física y finalmente dar clic en el botón "Registrar", y dicha conexión se grabara en el sistema.

1.2. Tab Enlaces

En el submenú "Enlaces" se pueden seleccionar 2 áreas de trabajo: Vrf y Vlan

1.2.1. Área de Trabajo Vrf

El área de trabajo Vrf tiene un grid donde se listan las vrf que han sido creadas en el sistema con la siguiente información de:

Nombre.- nombre de vrf

rt: route target

rd: route distinguisher

cliente: cliente para quien fue creada la conexión

estado: que puede ser;

Vrf creada.- indica que la vrf simplemente ha sido creada en el sistema pero aun no se utiliza en ninguna configuración

Vrf configurada.- significa que la vrf ya fue usada en alguna configuración en algún equipo



Vrf

Vlan

Listado de VRFs - capa 3

nombre	rd	rt	Cliente	Estado
clienteB	28025.2	28025.2	cliente B	Vrf Configurada
clienteL	28025.5	28025.5	cliente F	Vrf Creada
clienteA	28025.1	28025.1	cliente F	Vrf Configurada
vrfpaul	28025.77	28025.77	cliente F	Vrf Configurada

Agregar Eliminar Actualizar Aplicar VRF Salir

Fig A10: Vista – Área de trabajo de Vrf

En la figura A10 podemos apreciar el área de trabajo de "Vrf", la grilla de datos así como las opciones de configuración, en esta sección están disponibles las siguientes opciones:

Agregar una Vrf

Esta opción despliega la ventana (fig A11) donde el usuario debe ingresar la información de:

Nombre.- Nombre de la vrf

Route Target.- Propiedad de la vrf

Route Distinguisher.- Propiedad de la vrf

Tipo.- que puede ser:

- Transmisión de datos
- Internet Corporativo
- Internet Residencial

Cliente.- la ventana dispone de una grilla de clientes donde el usuario puede seleccionar el cliente para quien es creada la vrf



Registro de Vrf

Datos de registro.

Nombre: *

Route Distinguisher: *

Route Target: *

Tipo: * **Trasmision de datos** ▼

Clientes

Cliente: *

nombre	estado	Tipo
cliente A	1	corporativo
cliente B	1	residencial

Registrar **Salir**

Fig A11: Vista – Registro de Vrf

Ingresados todos los datos se da clic en el botón "Registrar" y se guarda en el sistema.

Eliminar una Vrf

Para la opción eliminar el usuario debe seleccionar previamente la vrf a ser eliminada y después dar clic en el botón. Una vrf que se encuentre en un estado "Vrf Configurada" no podrá ser eliminada ya que esta siendo usada en alguna configuración dentro del sistema.

Actualizar una Vrf

la grilla de Vrf tiene campos editables, es decir que el usuario esta en capacidad seleccionar el registro de vrf requerido, editar los campos y pulsar el botón Actualizar, al igual que en la eliminación esta opción solo esta disponible si la Vrf esta en un estado "Vrf Creada", caso contrario no se puede actualizar.



1.2.2. Área de Trabajo Vlan

El área de trabajo Vlan tiene un grid donde se listan las vlans que han sido creadas en el sistema con la siguiente información de:

Nombre.- nombre de vrf

tag: id de la vlan

descripción: descripción particular de la vlan

estado: que puede ser;

Activa.- indica que la vlan se utilizo en alguna configuración

Disponibile.- significa que la vlan fue creada en el sistema pero no se ha utilizado en ninguna configuración

Suspendida.- significa que la vlan ha sido dada de baja

The screenshot shows a web interface for managing VLANs. At the top, it says "Listado de Vlans - capa 3". Below this is a table with four columns: "nombre", "tag", "descripcion", and "Estado". The table contains four rows of data. Below the table, there are five buttons: "Agregar", "Eliminar", "Actualizar", "Aplicar Vlan", and "Salir".

nombre	tag	descripcion	Estado
myvlanA	23	vlan para clienteA	Disponibile
myvlanB	24	vlan para cliente B	Disponibile
myvlanC	47	para el cliente C	Disponibile
myvlanD	67	para el cliente D	Disponibile

Fig A12: Vista – Área de trabajo de Vlan

En la figura A12 podemos apreciar el área de trabajo de "Vlan", la grilla de datos así como las opciones de configuración, en esta sección están disponibles las siguientes opciones:

Agregar una Vlan



Esta opción despliega la ventana, figura A13, donde el usuario debe ingresar la información de:

Nombre.- Nombre de la vrf

Tag.- propiedad id única de cada vlan

Descripción-. Descripción particular de la vlan

The image shows a software window titled "Registro de Vlan" with a sub-window titled "Datos de registro.". The sub-window contains three text input fields, each preceded by a red asterisk (*). The labels for the fields are "Nombre:", "Descripcion:", and "Tag:". Below the input fields are two buttons: "Registrar" and "Salir". The window has a light green header bar with the text "vlan para clienteA" on the right side.

Fig A13: Vista – Registro de Vlan

Ingresados todos los datos se da clic en el botón "Registrar" y se guarda en el sistema.

Eliminar una Vlan

Para la opción eliminar el usuario debe seleccionar previamente la vlan a ser eliminada y después dar clic en el botón. Una vlan que se encuentre en un estado "Activa" o "Suspendida" no podrá ser eliminada ya que esta siendo usada en alguna configuración dentro del sistema.

Actualizar una Vlan



la grilla de Vlan tiene campos editables, es decir que el usuario esta en capacidad seleccionar el registro de vlan requerido, editar los campos y pulsar el botón Actualizar, al igual que en la eliminación esta opción solo esta disponible si la Vlan esta en un estado "Disponible", caso contrario no se puede actualizar.

1.3. Tab Configuraciones

En el submenú configuraciones se establecen los parámetros de una red mpls en los equipos, sus puertos físicos y virtuales. El área de trabajo de este submenú posee un listado de los equipos del sistema y las opciones de configuración como vemos en la figura A14, la grilla de equipos tiene la siguiente información de configuración:

Listado General de Equipos

Hostname	Jerarquia	MP-GBP	Mpls
PE_Z	Provider Edge - PE	No Activado	No Activado
PE_A	Provider Edge - PE	No Activado	Activo
P	Provider router - P	No Activado	No Activado

Puertos Vlans Habilitar BGP Habilitar Mpls Aplicar VRF Aplicar Vlan

Fig A14: Vista – Área de trabajo Tab Submenú Configuraciones

Hostname.- es el hostname del equipo

Jerarquía.- es la Jerarquía dentro de la Topología del dominio MPLS que puede ser P, PE, CE y RR (Route Reflector)



MP-BGP.- indica si el equipo tiene habilitado el protocolo BGP, opción valida solo para equipos de la Jerarquía PE

Mpls.- indica si el equipo tiene habilitado mpls de modo global

Las opciones que se encuentran en el área de trabajo en la parte inferior de la grilla de equipos se aplican de acuerdo al equipo que ha sido seleccionado en la grilla, a continuación especificamos las tareas funcionales que se pueden realizar en esta sección:

Para todas los procedimientos a continuación nos referiremos a la grilla de equipos ubicada en el submenú "configuración" del modulo de configuración con la etiqueta de Tab "Network"

Configuración Inicial Requerida

Antes de realizar cualquier configuración en los equipos lo primero es la configuración de la ip del puerto virtual loopback, todos los equipos del core MPLS deben tener configurada esta interfaz virtual para poder formar parte del dominio mpls y dado q es virtual es adecuada para el acceso al equipo para realizar configuraciones. Para realizar esto seguimos el siguiente procedimiento:

- Seleccionamos el equipo de la grilla
- Clic en el botón "puertos"
- Seleccionamos la interfaz loopback
- Editamos el campo de "Dirección ip", "Descripción IP" y escogemos la subred del combo en la columna "Subred".
- Damos clic en el botón "Aplicar IP", Ok al mensaje de confirmación y la ip queda aplicada al puerto



Una vez hecho esto podemos seguir con las configuraciones en los equipos.

Habilitar MPLS en un equipo de manera global

Este procedimiento habilita mpls en el modo de configuración global en un equipo del dominio MPLS determinado por el usuario.

- Seleccionamos el equipo de la grilla
- Damos clic en el botón "Habilitar MPLS"
- Se despliega una ventana de confirmación
- Dar clic en el botón "Ok"

Habilitar MPBGP en un equipo

Este procedimiento habilita mp-bgp en un equipo de jerarquía PE del dominio MPLS determinado por el usuario.

- Seleccionamos el equipo de la grilla
- Damos clic en el botón "Habilitar MP-BGP"
- Se despliega una ventana de confirmación
- Dar clic en el botón "Ok"

Aplicar una vlan en un equipo

Titulo de la ventana: Listado de Vlan - capa 3

nombre	tag	descripcion	Estado
myvlanA	23	vlan para clienteA	Disponible
myvlanB	24	vlan para cliente B	Disponible
myvlanC	47	para el cliente C	Disponible
myvlanD	67	para el cliente D	Disponible

Botones: Agregar, Eliminar, Actualizar, Aplicar Vlan, Salir



Fig A15: Vista – Listado de Vlans del Sistema

Este procedimiento aplica una vlan presente en el sistema en un equipo de jerarquía PE determinado por el usuario.

- Seleccionamos el equipo de la grilla
- Damos clic en el botón "Aplicar Vlans"
- Se despliega una ventana que contiene todas la vlans del sistema, el usuario debe seleccionar la vlan que desea aplicar al equipo, fig. A15
- Dar clic en el botón "Aplicar Vlan"

Aplicar una vrf en un equipo

nombre	rd	rt	Cliente	Estado
clienteB	28025:2	28025:2	cliente B	Vrf Configurada
clienteL	28025:5	28025:5	cliente F	Vrf Creada
clienteA	28025:1	28025:1	cliente F	Vrf Configurada
vrfpaul	28025:77	28025:77	cliente F	Vrf Configurada

Fig A16: Vista- Listado de Vrf's del Sistema

Este procedimiento aplica una vrf presente en el sistema en un equipo de jerarquía PE determinado por el usuario.

- Seleccionamos el equipo de la grilla
- Damos clic en el botón "Aplicar Vrf"
- Se despliega una ventana que contiene todas la vrf's del sistema, el usuario debe seleccionar la vrf que desea aplicar al equipo, fig A16



- Dar clic en el botón "Aplicar Vrf"

Puertos Físicos de un equipo

Los puertos físicos de un equipo representan las interfaces de red que posee y por las cuales se conecta a los demás equipos de la red, a continuación se especifican las tareas que se pueden realizar en sobre dichos puertos.

Como habilitar mpls en una interfaz

Mpls se puede habilitar en un interfaz para que el equipo empiece con el intercambio de etiquetas dentro del dominio mpls.

- Seleccionamos un equipo de la grilla
- Clic en el botón "Puertos"
- En la ventana que se despliega están listados todos los puertos del equipo (fig A17).
- Procedemos ha seleccionar el Puerto físico o Interfaz en la que deseamos habilitar mpls
- Clic en el botón "Habilitar Mpls"

Nombre	Descripcion de Int.	Tipo	Estado	Direccion Ip	Descripcion Ip	Subred	Mpls
e1/0/0	Interfaz. cris	GigaEthernet	Disponible				No Aplicable
e1/3	int4	GigaEthernet	Disponible			100.0.0.0	Active
e1/2	int3	GigaEthernet	Activa	10.1.1.5	int3	10.1.1.4	No Aplicable
e1/1	int2	GigaEthernet	Disponible	10.1.1.1	int2	10.1.1.0	No Aplicable

Fig A17: Vista – Listado de puertos de un Equipo



Como aplicar un ip en una interfaz física

Esta opción nos permite especificar la dirección ip en un puerto que forma parte del dominio mpls que ha sido configurada previamente de manera manual en un equipo

- Seleccionamos un equipo de la grilla
- Clic en el botón "Puertos"
- En la ventana que se despliega están listados todos los puertos del equipo (fig A17).

Seleccionamos el Puerto físico o Interfaz en la que deseamos aplicar la ip

- Editamos los campos "Dirección IP", "Descripción IP" y seleccionamos la subred del combo "Subred"
- Clic en el botón "Aplicar IP"

Como aplicar una vrf en un puerto físico

Esta opción valida solo para equipos de jerarquía PE nos permite aplicar una vrf con una dirección ip en un puerto que se configurará para conectarse a un CE

- Seleccionamos un equipo de la grilla
- Clic en el botón "Puertos"
- En la ventana que se despliega están listados todos los puertos del equipo (fig A17).

Seleccionamos el Puerto físico o Interfaz en la que deseamos aplicar la ip



- clic en el Botón "Vrf" ubicado en la esquina superior derecha de la ventana (fig A18). Con esta acción se visualiza una columna adicional de vrf en la grilla, esta columna adicional contiene un combo solamente de las vrf que han sido aplicadas en el equipo
- Editamos los campos "Dirección IP", "Descripción IP", seleccionamos la subred del combo "Subred" y seleccionamos la vrf del combo de vrf como vemos en la fig. A18
- Clic en el botón "Aplicar Vrf"

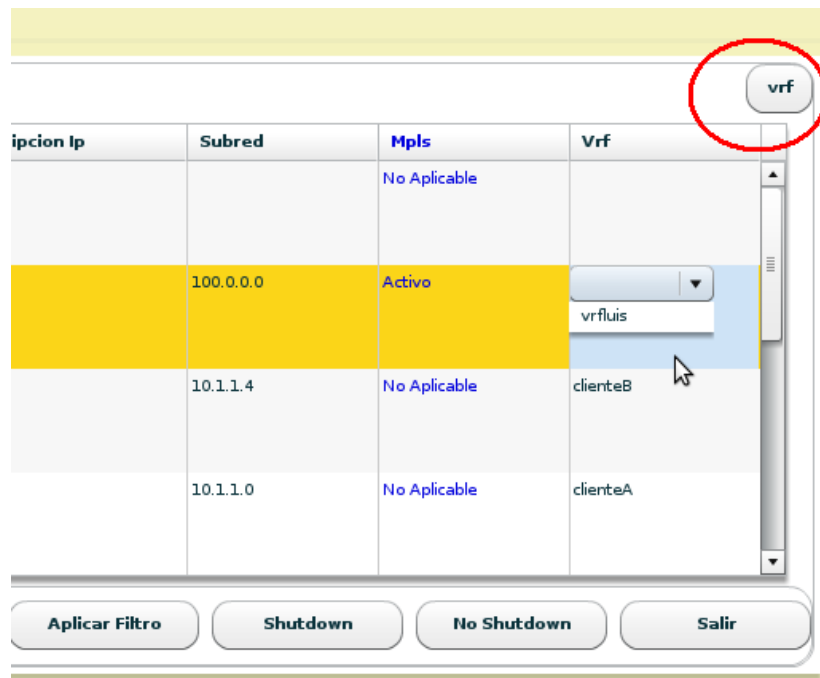


Fig A18: Vista – Selección de Combo Vrf – Botón Vrf

Hacer un shutdown de un puerto físico



Esta opción nos permite realizar shutdown en un puerto de un equipo seleccionado por el usuario

- Seleccionamos un equipo de la grilla
- clic en el botón "Puertos"
- En la ventana que se despliega están listados todos los puertos del equipo (fig A17).

Seleccionamos el Puerto físico o Interfaz

- clic en el botón "Shutdown"

Hacer un no shutdown a un puerto físico

Esta opción nos permite realizar No shutdown en un puerto de un equipo seleccionado por el usuario

- Seleccionamos un equipo de la grilla
- clic en el botón "Puertos"
- En la ventana que se despliega están listados todos los puertos del equipo (fig A17).

Seleccionamos el Puerto físico o Interfaz

- Clic en el botón "No Shutdown"

Como aplicar un filtro de vlan en un puerto físico de un equipo

Esta opción nos permite realizar el filtro de un vlan por un puerto de un equipo seleccionado por el usuario

- Seleccionamos un equipo de la grilla
- Clic en el botón "Puertos"
- En la ventana que se despliega están listados todos los puertos del equipo (fig A17).



- Seleccionamos el Puerto físico o Interfaz por el cual queremos aplicar el filtro, este puerto no debe formar parte del dominio mpls
- Clic en el botón "Vlans"
- En la ventana que se despliega están listados todos los vlans que han sido aplicadas al equipo previamente(fig A19).

Seleccionamos la vlan que queremos filtrar por el puerto anteriormente seleccionado

- Clic en el botón "Aplicar Filtro"

Nombre	Descripción	Tag	Estado	Dirección Ip	Descripción Ip	Subred	Vrf	Filtro
myvlanA	vlan para clienteA	23	Disponible			100.0.0.0	clienteB	No Disponible

Fig A19: Vista - Selección de Subred, Combo Subred

Vlans de un Equipos

Las vlans de un equipo se utilizan para representar los puertos virtuales de red del equipo, a continuación se especifican las tareas que se pueden realizar en sobre dichas vlans.

Como aplicar una vrf en una Vlan

Esta opción valida solo para equipos de jerarquía PE nos permite aplicar una vrf con una dirección ip en una vlan de un equipo

- Seleccionamos un equipo de la grilla



- Clic en el botón "Vlans"
- En la ventana que se despliega están listados todos los vlans del equipo (fig A19).
- Seleccionamos vlan en la que deseamos aplicar una vrf
- Editamos los campos "Dirección IP", "Descripción IP", seleccionamos la subred del combo "Subred" y seleccionamos la vrf del combo de vrf, las vrf que se desplieguen en el combo serán solamente las que han sido aplicadas previamente en el equipo.
- Clic en el botón "Aplicar Vrf"

Como hacer shutdown a nivel de vlan

Esta opción nos permite realizar shutdown en una vlan de un equipo seleccionado por el usuario

- Seleccionamos un equipo de la grilla
- Clic en el botón "Vlans"
- En la ventana que se despliega están listados todos las vlans del equipo (fig A19). Seleccionamos la vlan.
- Clic en el botón "Shutdown"

Como hacer shutdown a nivel de puerto

Esta opción nos permite realizar Shutdown de una vlan a nivel de puerto virtual en un equipo seleccionado por el usuario

- Seleccionamos un equipo de la grilla
- Clic en el botón "Puertos"
- En la ventana que se despliega están listados todos los puertos del equipo (fig A17).
- Seleccionamos el Puerto físico o Interfaz



- Clic en el botón "Vlans"
- En la ventana que se despliega están listados todos los vlans del equipo (fig A19).
- Seleccionamos la vlan de la grilla
- Clic en el botón "Shutdown"

Como hacer No shutdown a nivel de vlan

Esta opción nos permite realizar No shutdown en una vlan de un equipo seleccionado por el usuario

- Seleccionamos un equipo de la grilla
- Clic en el botón "Vlans"
- En la ventana que se despliega están listados todos las vlans del equipo (fig A19). Seleccionamos la vlan.
- Clic en el botón "No Shutdown"

Como hacer "No shutdown" a nivel de puerto

Esta opción nos permite realizar No shutdown de una vlan a nivel de puerto virtual en un equipo seleccionado por el usuario

- Seleccionamos un equipo de la grilla
- Clic en el botón "Puertos"
- En la ventana que se despliega están listados todos los puertos del equipo (fig A17).
- Seleccionamos el Puerto físico o Interfaz
- Clic en el botón "Vlans"
- En la ventana que se despliega están listados todos los vlans del equipo (fig A19).
- Seleccionamos la vlan de la grilla



- Clic en el botón "No shutdown"

The screenshot shows a web interface for managing equipment. At the top, there are tabs for 'Equipos' and 'Respaldo'. Below the tabs is the title 'Listado General de Equipos' and a button labeled 'Ubicacion'. The main content is a table with the following data:

Hostname	Jerarquía	Tipo	Marca	Modelo
PE_Z	Provider Edge - PE	Swiich Cisco	Cisco	Swiich
PE_A	Provider Edge - PE	router	cisco	7604
P	Provider router - P	router	cisco	7609

At the bottom of the interface, there are five buttons: 'Agregar', 'Eliminar', 'Actualizar', 'Respaldar', and 'Agregar Puerto'.

Fig A20: Vista - Área de Trabajo, Modulo Equipos

2. Modulo de Equipos

En este modulo el usuario podrá realizar la gestión de los equipos del sistema, el área de trabajo nos presenta una grilla con información del equipo como vemos en la figura A20, el botón "ubicación" en la esquina superior derecha despliega columnas en la grilla con información de la ubicación de los equipos como vemos en la figura A21.



equipos

Modelo	Sector	Edificio	Latitud	Longitud	Ubicación
Switc	oeste	oeste	-2.8971824447109	-78.978244229888	
7604	este	este	-2.8997540712931	-79.017554685211	
7609	centro	centro	-2.8997540712931	-78.999444409942	

Fig A21: Vista - Botón Ubicación, Área de trabajo Equipos

Ingresar equipos al Sistema

Esta opción nos permite agregaron equipo al sistema que será graficado en el mapa de google



Registro de Equipo

Datos de registro.

Nombre: * Jerarquía: * **Provider router - P** ▼

Descripción: *

Cuenta de administración del equipo:

Login: * Clave: *

Información de la ubicación:

Sector: * Edificio: *

Latitud: * Longitud: *

Descripción: *

Tipo: * **Tipo Equipos** ▼

Interfaces: *

Nombre	Descripción	Tipo
lo1	Interfaz Loopback	Loopback ▼
Click to add item...		FastEthernet ▼

Fig A22: Vista – Registro de Equipos

- Clic en el botón "Agregar"
- En la ventana que se despliega podemos ingresar los valores del nuevo equipo a ser ingresado en el sistema. figura A22
- Ingresamos la información:
 - Nombre.- es el hostname del equipo
 - Descripción.- descripción particular del equipo
 - Jerarquía.- Jerarquía del equipo dentro del dominio mpls (P, PE, CE, RR)
 - Login.- nombre del usuario administrador del equipo
 - Clave.- clave del usuario administrador del equipo
 - Sector.- información de ubicación del equipo
 - Edificio.- información de ubicación del equipo



- Latitud.- coordenadas de latitud, ubicación del equipo
 - Longitud.- coordenadas de longitud, ubicación del equipo
 - Descripción.- descripción, ubicación del equipo.
 - Tipo Equipo.- el tipo de Equipo que escojamos también determinara el icono que tendrá el equipo en el mapa de google
 - Interfaces.- En grilla ubicado en la parte inferior en la figura A22, se tiene que ingresar las interfaces o puertos físicos del equipo, incluyendo los siguientes datos
 - interfaz-Nombre.- Nombre de la Interfaz
 - Interfaz-Tipo.- Tipo de Interfaz del equipo que puede ser Giga/Fast Ethernet
 - Interfaz-Descripción.- La descripción de la interfaz.
- Clic en el botón "Registrar".

Actualizar un equipo

La grilla de Equipos tiene campos editables, es decir que el usuario esta en capacidad de seleccionar el registro de equipo requerido, editar los campos y pulsar el botón "Actualizar", esta opción solo esta disponible si el equipo esta en un estado "Disponible", caso contrario no se puede actualizar.

Eliminar un equipo

Para la opción eliminar el usuario debe seleccionar previamente el equipo a ser eliminado y después dar clic en el botón "Eliminar". Una Equipo que se encuentre en un estado "Configurado" no podrá ser



eliminado ya que esta siendo usada en alguna configuración dentro del sistema.

Agregar Puertos físicos o interfaces en un equipo

La opción de agregar nuevas interfaces físicas al equipo se realiza el siguiente procedimiento.

- Seleccionar el equipo al cual queremos agregarle las interfaces
- Clic en el botón "Agregar Puerto"
- En la ventana que se despliega como vemos en la figura tenemos un grid donde podemos agregar nuevas interfaces para el equipo
- Ingresadas las interfaces damos clic en el botón "Registrar"

3. Modulo de Utilidades de Red

Traceroute Nslookup Ping

Ping: comprobar el estado de la conexión

Domain o ipaddress: * 192.168.1.1 TimeOut(ms): * 1000

Paquetes a enviar: * 5 ttl(hops): * 255

data size (bytes): * 32

Ping

Pinging dominio [ip] with 32 bytes of data...

resultado...

Fig A23: Vista – Área de Trabajo, Submenú Ping, Modulo Utilidades de Red



Esta utilidad de red se utiliza para tareas de operación para verificar conectividad con los equipos que forman parte de la red y examinar que no existan pérdidas de paquetes. la figura A23 muestra el área de trabajo del utilidad ping. En el recuadro "Domain o IPaddres" ingresamos la ip o dominio a la cual queremos hacer ping y damos clic en el botón "Ping"

Traceroute

Esta utilidad de red se utiliza para tareas de operación para verificar conectividad con un seguimiento de los saltos de red que se llevan a cabo para llegar a un destino. La figura A24 muestra el área de trabajo de la utilidad traceroute.

En el recuadro "A: " ingresamos la ip o dominio a la cual queremos hacer traceroute, en el combo de la opción desde escogemos el equipo desde el cual queremos hacer el traceroute.

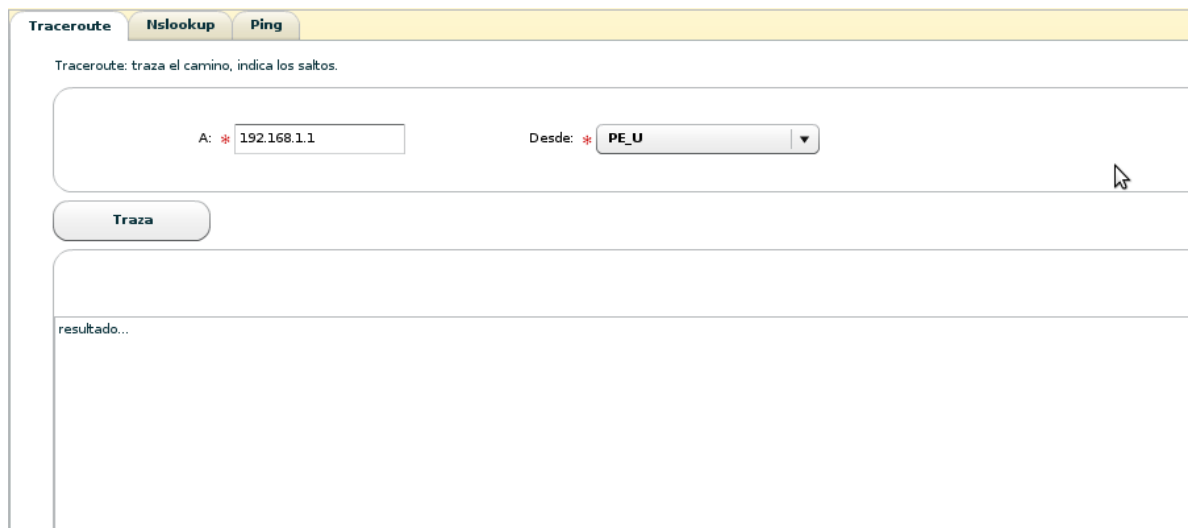


Fig A24: Vista – Área de Trabajo, Submenú Traceroute, Modulo Utilidades de Red

Nslookup



Esta utilidad de red se utiliza para tareas de consulta de dominios y direcciones ip versión 4. La figura A25 muestra el área de trabajo de la utilidad nslookup. En el recuadro "Domain" ingresamos la ip o dominio a la cual queremos hacer nslookup y damos clic en el botón "Nslookup"

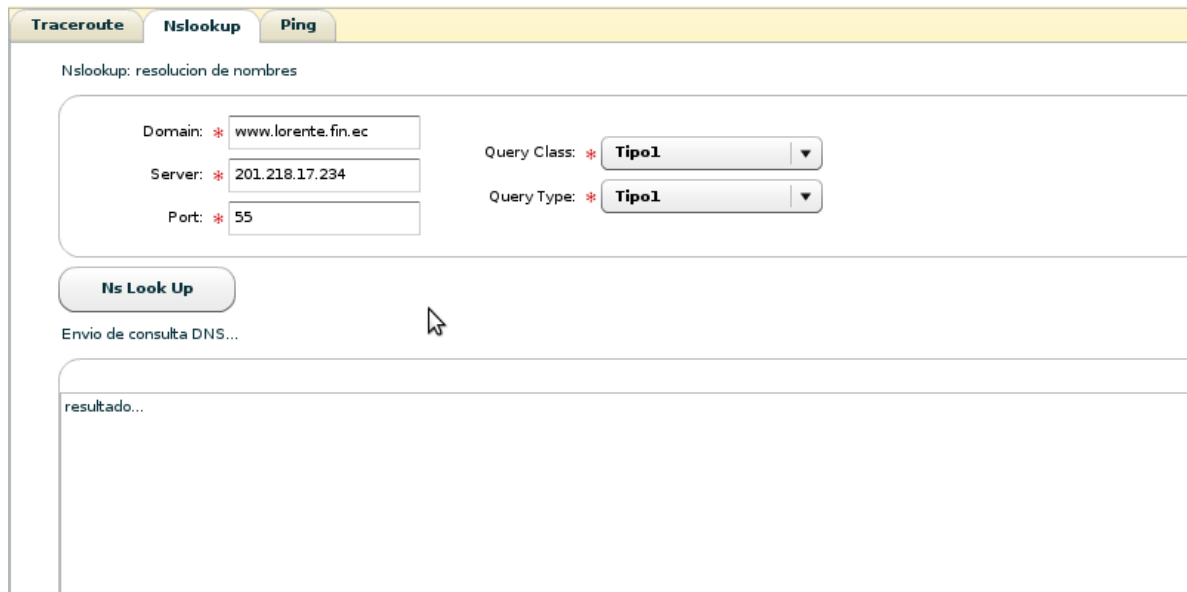


Fig A25: Vista – Área de Trabajo, Submenú Nslookup, Modulo Utilidades de Red

4. Modulo de Vism

El modulo de Vism IPv4 es donde el usuario puede gestionar la información de capa de red del dominio mpls, esta información es de utilidad en la configuración de los equipos de la red. en la figura A26 vemos el área de trabajo del modulo Vism. A continuación se listan las funcionalidades del modulo:



NETWORK EQUIPOS UTILITIES VLSM IPV4 CLIENTES USUARIOS MONITOREO CONSOLA VIRTUAL

Direccionamiento IP

Descripcion: *

Direccion Ip: * 1 0 0 0

Numero de hosts: * 1

Ubicacion: * Nodo 3
 Nodo 4
 Nodo 5
 Core

Ip ingresada:
IP de Red:
Mascara:
Broadcast:
-# Ips disponibles:

Subredes Calculadas

descripcion	ipred	mascara	broadcast	Ips disponibles	Ips utilizadas	nodo	estado
subred del cliente A	10.1.1.0	255.255.255.252	10.1.1.3	2	1	3	1 Ips libres.
loop p	172.16.1.1	255.255.255.255	172.16.1.1	1	1	3	Ocupada
conexion pa_a	192.168.1.0	255.255.255.252	192.168.1.3	2	2	0	Ocupada

Eliminar

Fig A26: Vista – Área de Trabajo, Modulo Vism

Calcular una Subred

En el área de trabajo del módulo Vism figura A26, procedemos del a siguiente manera:

- Ingresamos la 4 octetos en formato decimal de la Dirección IP v4
- Indicamos el número de hosts que queremos en la subred
- Clic en el botón "Calcular"
- La información genera del Calculo se publica en la sección superior derecha del área de trabajo

Como agregar una Subred al sistema

- Ingresamos la Descripción de la Dirección IP v4
- Calculamos la subred
- Escogemos el nodo al cual va a pertenecer la subred
- Clic en el botón "Guardar"

Como eliminar una subred del sistema

- Seleccionamos la subred de la grilla presente en el área de trabajo de Vism, figura A26
- Clic en el botón "Eliminar"



Solamente se podrá eliminar subredes que estén en un estado con cero IPs ocupadas.

5. Modulo Usuarios

El modulo de Usuarios gestiona la información de los usuarios del sistema, el área de trabajo del modulo de usuarios se observa en la figura A27 quien cuenta con una grilla donde se listan los usuarios del sistema, a continuación se listan las tareas que se pueden realiza en este modulo.

Login	Rol	E-mail	Empleado
admin	Administrador Sistema	admin@siam.com	empleadoA
demo	Administrador Red	demo@siam.com	empleadoB
aux	Operador	aux@siam.com	empleadoC

Agregar Eliminar Actualizar

Fig A27: Vista – Área de Trabajo, Modulo Usuarios

Crear un Usuarios del sistema

Esta opción del módulo permite crea nuevos usuarios para el sistema, procedimiento:

- Clic en el botón “Agregar”
- En la ventana que se despliega (figura A28) se ingresa la información del nuevo usuario:
 - Nombre.- nombre del usuario
 - Clave.- Clave para el usuario dentro del sistema



- Email.- dirección de correo corporativo de la empresa
- Rol.- es el rol del empleado que puede ser:
 - Administrador del Sistema
 - Administrador de la Red
 - Operador
- Empleado.- seleccionamos el empleado del departamento de la dirección de telecomunicaciones para el cual se esta creando el usuario
- Clic en el botón “Registrar”

Eliminar un Usuario del Sistema

- Seleccionamos el usuario de la grilla presente en el área de trabajo del modulo Vism, figura A27
- Clic en el botón “Eliminar”

Actualiza un Usuario del Sistema

La grilla de “Usuarios” tiene campos editables, es decir que el usuario del sistema esta en capacidad de seleccionar el registro de “usuario” requerido, editar los campos y pulsar el botón “Actualizar”.



Registro de Usuario
MONITOREO CONSOLA VIRTUAL

Datos de registro.

Usuario: *

Clave: *

Email: *

Rol: * Roles

Empleado: *

Nombre	Estado
empleadoA	1
empleadoB	1
empleadoC	1
empleadoD	1

Registrar Salir

Fig A28: Vista – Área de Trabajo, Registro Usuarios, Modulo Usuarios

6. Modulo Clientes

El modulo de Clientes presenta información de los clientes de Centronet, información q es publicada en el sistema para tareas de administración en los módulos de configuración. La figura A29 nos muestra el área de trabajo del modulo de clientes donde observamos una grilla informativa de los clientes con un filtro según el tipo ya este corporativo o residencial.

NETWORK | EQUIPOS | UTILITIES | VLSM IPV4 | CLIENTES | USUARIOS | MONITOREO | CONSOLA VIRTUAL

Clientes

nombre	Estado	Tipo
cliente A	Activo	corporativo
cliente B	Activo	residencial
cliente C	Activo	corporativo
cliente D	Activo	residencial



Fig A29: Vista – Área de Trabajo, Modulo Clientes

Manual del Sistema

1. Instalación del Servidor

El Servidor Considerado para el sistema es GNU/Linux en su versión Centos 5.5 derivada de su par comercial Red Hat. Previo a la instalación se realiza un análisis de requerimientos que el servidor utilizar en su ejecución considerando un periodo de crecimiento de los recursos requeridos por la aplicación. Al tratarse de un sistema prototipo estas estimaciones se limitaron a la disponibilidad de la maquina proporcionada.

Proceso de Instalación

Insertamos el disco de instalación en el CD-ROM del Servidor Blade HP



Fig A30: Pantalla de bienvenida

Reiniciamos el equipo y al encenderse se nos presentara la pantalla como se indica en la figura A30 donde escribimos Linux text y proseguimos con el proceso de instalación con el wizard Anaconda.



El wizard nos ofrece varias alternativas como: Revisión del Disco de instalación, selección del idioma de instalación, que se seleccionan según la preferencia del usuario q instala el servidor.

Para este proceso de instalación previamente se debe contar con una planificación que brinde información de:

Particionamiento de Disco Duros

Información de contraseñas de root

Direccionamiento IPv4

Configuración de Dominio

Dado que la maquina esta dedicada como servidor hospedero de la aplicación, se utilizara el Grub predeterminado para el arranque del sistema operativo:

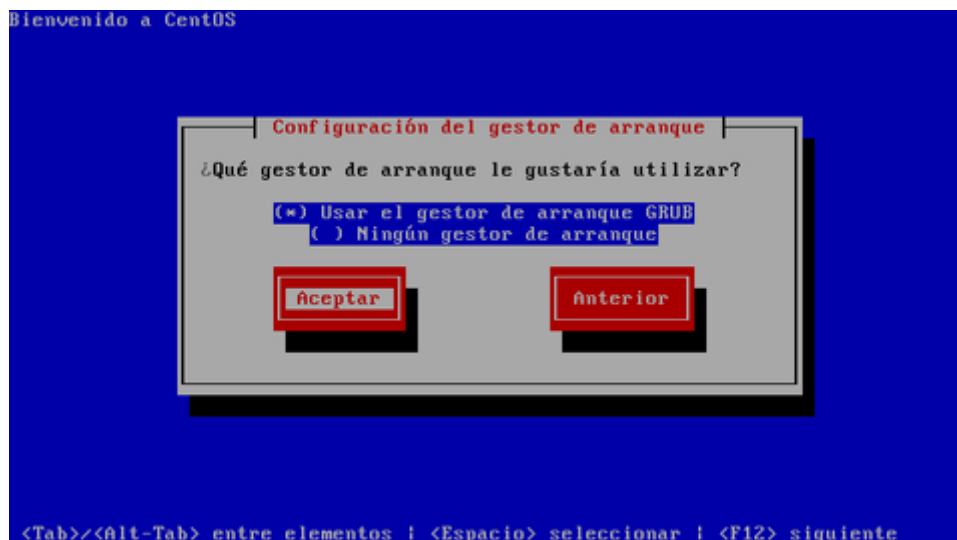


Fig A31: Selección de Gestor de Arranque

En la configuración de los parámetros de red activamos el soporte de IPv4, especificamos el dirección IPv4 y mascara para la subred en este caso eth0



Fig A32: Configuración de los parámetros de red

Configuramos los parámetros de Gateway y DNS.



Fig A33: Configuración de los parámetros de red

Se especifican los parámetros de hostname, Uso horario y seleccionamos los paquetes Base del Servidor Centos ya que las herramientas de software se instalaran de maneta manual.

Propiedades del Servidor

Hostname

```
root@nms:~# hostname -a
```



Universidad de Cuenca

nms nms.centronet.net.ec

Memoria

A continuación se detalla una consulta de memoria que se ejecuto con el servidor en estado operativo pero carga de procesamiento

```
root@nms:~# free -m
```

		total	used	free	shared	buffers	cached
Mem:	990	270	720	0	97	98	
Swap:	551	0	551				

Como se puede ver la memoria RAM es de 1GB, con un total de 270Mb ocupados y 720Mb libres.

Procesador

A continuación se detalla información del procesador

```
vendor_id           : GenuineIntel
cpu family          : 6
model               : 23
model name          : Intel(R) Xeon(R) CPU           X5450  @
3.00GHz
stepping            : 6
cpu MHz             : 2999.855
cache size          : 6144 KB
cpuid level         : 4
bogomips            : 5999.71
clflush size        : 64
```



Direccionamiento IP

Según el modelo de trabajo de Centronet para publicar un servidor a la Web se utiliza

Interfaz	Dirección IP	Mascara	IP Red	Nat
Eth0	192.168.27.60	255.255.255.192		190.120.76.133

Kernel

```
root@nms:~# uname -r
```

```
2.6.31-14-generic-pae
```

Almacenamiento

Es así que se ha seleccionado un modelo de Volúmenes Lógicos con LVM a partir del Espacio de almacenamiento físico del cual dispone el Server ya que brindara la capacidad de extensiones a futuro, aplicando la siguiente configuración al Servidor NMS:

```
root@nms:~# vgdisplay
```

```
--- Volume group ---
```

```
VG Name          servertesis
```

```
System ID
```

```
Format          lvm2
```

```
Metadata Areas   1
```

```
Metadata Sequence No 3
```

```
VG Access        read/write
```

```
VG Status        resizable
```



Universidad de Cuenca

```
MAX LV          0
Cur LV         2
Open LV        2
Max PV         0
Cur PV        1
Act PV         1
VG Size        11,76 GB
PE Size        4,00 MB
Total PE       3010
Alloc PE / Size 3003 / 11,73 GB
Free PE / Size  7 / 28,00 MB
VG UUID        7Y3oFV-9qKy-rBi7-IT3Q-w6HI-2GPU-Cjezo2
```

root@nms:~# lvdisplay

--- Logical volume ---

```
LV Name          /dev/servertesis/root
VG Name          servertesis
LV UUID          m42zMX-Ge0r-v8I2-KF6R-KiNT-h41V-EMvYYC
LV Write Access  read/write
LV Status        available
# open           1
LV Size          11,19 GB
Current LE       2865
Segments         1
Allocation       inherit
Read ahead sectors auto
```



Universidad de Cuenca

- currently set to 256

Block device 252:0

--- Logical volume ---

LV Name /dev/servertesis/swap_1

VG Name servertesis

LV UUID 6hbVt5-sRZR-9F92-XPfh-2BTd-wzWJ-KqJ8nz

LV Write Access read/write

LV Status available

open 2

LV Size 552,00 MB

Current LE 138

Segments 1

Allocation inherit

Read ahead sectors auto

- currently set to 256

Block device 252:1

2. Instalación de Base de Datos

Para la Instalación de Mysql se ingresa como root a la terminal del servidor y digitamos:

```
yum -y install mysql mysql-server
```

Aparte se tiene que habilitar los permisos para el funcionamiento correcto de Mysql en SELinux, digitamos el siguiente comando

```
# setsebool -P mysqld_disable_trans 1
```

```
# setsebool -P allow_user_mysql_connect 1
```



Tarea que también podemos hacerla de manera grafica abriendo un escritorio gnome con el comando:

```
# startx
```

Y digitando en un terminal:

```
# system-config-securitylevel
```

Con lo que se nos abre una ventana de dialogo con la que podemos permitir el servicio mysql con un simple clic.

Podemos comprobar la ejecución del servicio con el siguiente comando:

```
# netstat -nat|grep 3306
```

Ahora procedemos a cambiar clave de root y darle acceso a mysql, para esto procedemos de la siguiente manera:

Detenemos el servicio de MySQL

```
/etc/init.d/mysql stop
```

Saltamos los privilegios de MySQL

```
/usr/bin/mysqld_safe --user=mysql --skip-grant-tables
```

Abrimos otra terminal y escribimos

```
mysql
```

Con esto ya estamos dentro de la Base de Datos por lo tanto usamos la base de datos llamada mysql

```
use mysql;
```

Actualizamos el campo Password del usuario root de la siguiente manera

```
UPDATE user SET Password=PASSWORD('nuestro_password') WHERE user='root';
```

Salimos

```
exit;
```



Iniciamos una nueva sesión en la base de datos desde la terminal

```
mysql -u root -p
```

y tendremos que meter nuestro password.

Ahora tenemos la capacidad de administrar la Base de Datos con lo que procedemos a crear una Base de Datos con la siguiente sentencia.

```
# mysqladmin -u root -p "nombre_BD"
```

La propiedad nombre nombreBD para el presente proyecto es "tesisbd"

Una vez creada la base de datos ejecutar el script tesisbd.sql para cargar todas las tablas de la base de datos, esto lo realizamos de la siguiente manera.

```
mysql -u root --password="la_clave" < tesisbd.sql
```

3. Instalación del Servidor Web

Instalación de Java

```
# yum install sun-java6-plugin sun-java6-jdk
```

Especificamos nuestro java Home para que después pueda ser encontrado por el servidor Tomcat, editamos el siguiente fichero:

```
# vim /usr/local/tomcat6/apache-tomcat-6.0.26/bin/catalina.sh
```

Y Agregamos la siguiente línea al final del fichero.

```
JAVA_HOME=/usr/lib/jvm/java-6-sun
```

La segunda opción para realizar esto es editando el siguiente fichero

```
# vim /root/.bashrc
```

Y así también agregamos al final la siguiente línea:

```
export JAVA_HOME=/usr/lib/jvm/java-6-sun
```

Instalación de Tomcat



Para la configuración del Tomcat Editamos el siguiente fichero para establecer la clave de Administración del servidor

```
# vim /usr/local/tomcat6/tomcat-users.xml
```

Procedemos a editar el fichero con la siguiente información

```
<role rolename="manager"/>
```

```
<role rolename="admin"/>
```

```
<user name="root" password="la_clave" roles="manager,admin"/>
```

4. Instalación de los Paquetes de Software

Instalación de la herramienta expect

```
# yum install expect
```

Instalación de Servidor telnetd

```
# yum install telnetd
```

```
# /etc/init.d/openbsd-inetd restart
```

Instalar de la herramienta traceroute

```
# yum install traceroute
```

5. Instalación del Servidor TFTP

```
# yum install vsftpd
```

Para este servidor podemos realizar varias configuraciones de seguridad como enjaulamiento de usuarios entre otros, que se dejaran a consideración del administrador. La instalación por defecto posee los requerimientos para las funcionalidades del presente proyecto.

6. Instalación de la Aplicación

La aplicación se empaqueta en un fichero de extensión .war valido y compatible con Tomcat quien realiza el deploy o despliegue de fichero



generando el subdirectorío del mismo nombre del fichero bajo el directorío webapps, por lo que el proceso a realizar es copiar el fichero en el directorío. Para el caso del presente proyecto la ubicación del directorío es:

`/usr/local/tomcat6/apache-tomcat-6.0.29/webapps`

7. Configuración del Navegador del cliente web

La única configuración que se requiere del lado del usuario final es el afinamiento del navegador web que requiere la Instalación de flashplayer en su versión 10 o superiores algo que actualmente lo maneja la mayoría de los usuarios para navegar en internet siendo este un estándar de facto.

4.6 BIBLIOGRAFÍA

Tema: MPLS VRF

[1] VPN Routing and Forwarding Tables

http://www.cisco.com/en/US/docs/net_mgmt/vpn_solutions_center/1.1/user/guide/VPN_UG1.html#wp1018964

[2] MPLS VPN, Configuración de Red MPLS

http://www.rasyid.net/wp-content/uploads/2007/11/mpls_tut.pdf

Tema: Modelo Jerárquico Cisco

[3] Cisco, Core distribución y acceso

<https://learningnetwork.cisco.com/message/119715>

[4] Wordpress, Core distribución y acceso

<https://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/>

[5] Apendicular, Modelo Jerárquico Cisco

<http://aprenderedes.com/2006/06/las-tres-capas-del-modelo-jerarquico-de-cisco/>



Tema: Aplicaciones RIA

[5] Adobe Labs, Flex livedocs

http://livedocs.adobe.com/flex/3/html/help.html?content=controls_08.html

[6] Google code, Flex Windows Manager

Flex - manejo de ventanas:

<http://code.google.com/p/flexmdi/>

[7] Adobe Labs, Flex Windows Example

<http://benclinkinbeard.com/flexmdi/explorer/>

Tema: SNMP

[8] Arcesio, ASN

<http://www.arcesio.net/osinm/asn1.html>

[9] Wikipedia, MIB

http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol

[10] Siemens Support, MIB

<http://support.automation.siemens.com/WW/llisapi.dll/15177711?func=ll&objId=32447945&objAction=csView&lang=es&siteid=cseus&aktprim=0&extraneat=standard&viewreg=WW&load=treecontent>

[11] WebNMS, API SNMP java

<http://www.webnms.com/snmp/help/gettingstarted/index.html>

[12] WebNMS, Framework Guide

http://www.webnms.com/webnms/help/quick_tour/index.html

[13] WebNMS, API Information

http://www.webnms.com/snmp/snmpapi_datasheet.html#comparison

[14] WebNMS, package structure

<http://www.webnms.com/snmp/help/gettingstarted/index.html>

[15] WebNMS, download



<http://www.webnms.com/snmp/download.html>

[16] SaS, Overview of SAS Application

<http://support.sas.com/documentation/cdl/en/biasag/61237/HTML/default/viewer.htm#/documentation/cdl/en/biasag/61237/HTML/default/a003135494.htm>

Tema: Network Management System

[17] Albiore, MRTG

<http://albiore.com/es/mrtg>

Tema: FCAPS

[18] Networld, FCAPS

<http://www.networkworld.com/details/6184.html>

[19] Integrared, FCAPS

<http://integrared.blogspot.com/2009/07/las-cinco-capas-funcionales-de-la.html>

[20] Wikipedia, FCAPS

<http://es.wikipedia.org/wiki/FCAPS>

Tema: Expect

[21] Sourceforge, Expect

<http://expect.sourceforge.net/>

[22] Sourceforge, ExpectJ

<http://expectj.sourceforge.net/>

Tmea: GNS3

[23] GNS3, software

<http://www.gns3.net/>

[24] GNS3, integracion VMware

<http://www.gns3.net/phpBB/topic1139.html?sid=b38c6c49948bf25cbc322e698cb220d1>

[25] Conft, IOS cisco routers



http://confit.com/en/US/docs/routers/7200/technical_references/7200_mib_guides/7200_mib_specs_guide_v3/7200mib2.html

[26] Cisco, equipos de red

http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheets_list.htm<http://www.cisco.com/en/US/products/hw/routers/ps368/ps367/index.html>

<http://www.cisco.com/en/US/products/ps5856/index.html>

http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheets_list.htm
