FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

"INTEGRACIÓN DE LA MATERIA LABORATORIO DE TELEMÁTICA PARA LA FACULTAD TÉCNICA USANDO EL SIMULADOR GRÁFICO DE REDES GNS3"

Previo a la obtención del título de
INGENIERO EN TELECOMUNICACIONES
MENCIÓN EN GESTIÓN EMPRESARIAL

Elaborado por:

Mario Javier Gil Cevallos

Verónica Paola Berruz Silva

Director de Tesis

Ing. Jorge Abraham Rosero Moreno

Guayaquil, 23 de Septiembre del 2013

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por el Sr. Mario Javier Gil Cevallos y la Srta. Verónica Paola Berruz Silva como requerimiento parcial para la obtención del título de INGENIERO EN TELECOMUNICACIONES.

Guayaquil, 23 de Septiembre del 2013

DIRECTOR:

_____
Ing. Jorge Abraham Rosero Moreno

REVISOR:

_____
Ing. Luzmila Ruilova Aguirre

REVISOR:

_____
Ing. Manuel Romero Paz

DIRECTOR DE CARRERA:

_____
Ing. Miguel Armando Heras Sánchez

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Mario Javier Gil Cevallos y Verónica Paola Berruz Silva

DECLARAMOS QUE:

El proyecto de grado denominado "Integración de la materia Laboratorio de Telemática para la Facultad Técnica usando el Simulador Gráfico de Redes GNS3", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de nuestra total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico de la tesis del grado académico en mención.

Guayaquil, 23 de Septiembre del 2013

AUTORES:

_____
Mario Javier Gil Cevallos

_____
Verónica Paola Berruz Silva

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Mario Javier Gil Cevallos y Verónica Paola Berruz Silva

Autorizamos a la Universidad Católica de Santiago de Guayaquil, la publicación en la biblioteca de la institución del proyecto titulado: "Integración de la materia Laboratorio de Telemática para la Facultad Técnica usando el Simulador Gráfico de Redes GNS3", cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Guayaquil, 23 de Septiembre del 2013

AUTORES:

_____
Mario Javier Gil Cevallos

_____
Verónica Paola Berruz Silva

Agradecimiento

Nuestro agradecimiento a Dios, por llevarnos a su lado a lo largo de esta vida, siempre llenándonos de fortaleza y dicha y, por dejarnos culminar con éxito nuestros propósitos de ser profesionales.

A nuestros padres, por enseñarnos los valores y toda la fuerza, por el constante apoyo y paciencia.

Igualmente, queremos agradecer cordialmente a las autoridades de la Facultad Técnica, en especial a nuestro director de tesis por su voluntad, esfuerzo, dedicación y apoyo durante la realización de nuestra tesis.

También nos gustaría agradecer los consejos y reflexiones recibidos a lo largo de los últimos años a todos los profesores de la Facultad Técnica que tuvimos mientras cursábamos la carrera de telecomunicaciones, y que de una manera u otra han aportado con el conocimiento valioso para culminar con éxito este trabajo de tesis.

Dedicatoria

Esta tesis está dedicada especialmente a nuestros padres, por su comprensión y ayuda en momentos malos y buenos. Quienes nos han enseñado a encarar las adversidades sin perder nunca la fe, quienes con sus ejemplos y buenos deseos, se pudo triunfar y alcanzar un título profesional.

Son nuestros padres quienes nos han dado todo lo que somos como persona, los valores, principios, perseverancia y empeño, y todo ello con una gran dosis de amor y sin pedir nunca nada a cambio.

Igualmente, este trabajo está dedicado a todos los estudiantes de la Facultad Técnica de la carrera de Telecomunicaciones.
A todos nuestros profesores y autoridades de la Facultad Técnica, por la comprensión, apoyo incondicional y consejos, a todos ellos, está dedicada esta tesis.

Resumen

El presente trabajo de graduación contempla el estudio de los diferentes escenarios que se pueden crear con un simulador gráfico de redes de alto nivel como lo es GNS3, y que por medio de este se pueda interactuar con routers físicos y PC's no solo virtuales sino también reales aplicando conocimientos previamente obtenidos en las materias de Telemática I y II; el objetivo de esta propuesta de integración de la materia es la formación de los mismos estudiantes, ya que estos obtendrán un mejor criterio en cuanto al área del networking y TI's (Tecnologías de información); y como el mundo de las telecomunicaciones es sumamente extenso y siempre está en constante avance, es por este motivo la justificación para la realización de este trabajo de investigación y proponer de que se integre la materia Laboratorio de Telemática.

En la tesis se presenta en el capítulo 2, una fundamentación teórica en lo que concierne al simulador GNS3 y todas sus características, además de cómo usarlo y explicación de los requerimientos para poder realizar prácticas en este simulador, en el capítulo 3 trataremos acerca de todas las tecnologías que se pueden simular con GNS3, este es un capitulo muy importante ya que estas tecnologías a tratar en este capítulo son las que finalmente se trataran de ejecutar en las creación de los escenarios para las prácticas del laboratorio y a su vez estas se las encontraran profesionalmente en cualquier trabajo de telecomunicaciones, en el capítulos 4 se presenta el diseño metodológico para la integración de la materia, aquí se creara un pensum en la cual se integre la materia Laboratorio de Telemática en la carrera de Ingeniería en Telecomunicaciones, además de una planificación del curso propiamente dicho y la creación de cada uno de los escenarios para las prácticas del laboratorio, este proceso de la creación de escenarios será sumamente investigativo y en el capítulo 5 un presupuesto aproximado de lo que costará la integración de esta materia en la Facultad de Educación técnica para el desarrollo.

De esta manera se cumple el objetivo planteado en esta tesis que era presentar una propuesta para integración de un Laboratorio de Telemática la cual es un buen complemento de las clases teóricas de Telemática I y II, y esta les permitirá a los estudiantes consolidar todos sus conocimientos en el área del networking y poder aplicar a mejores ofertas laborales en el ámbito profesional.

ÍNDICE GENERAL

CAPÍTULO 1 ..... - 14 -
DISEÑO DEL TRABAJO DE TITULACIÓN ..... - 14 -
1.1. Introducción - 14 -
1.2. Justificación - 15 -
1.3. Planteamiento del Problema - 16 -
1.4. Objetivo General - 16 -
1.5. Objetivos Específicos - 17 -
1.6. Hipótesis - 17 -
1.7. Metodología de Investigación - 17 -
CAPÍTULO 2 ..... - 18 -
FUNDAMENTOS TEORICOS ..... - 18 -
2.1. Laboratorio de Telemática - 18 -
2.1.1. Introducción - 18 -
2.1.2. El uso de dispositivos IP en ISP's y redes locales - 19 -
2.1.3. Routing en un entorno de Proveedor de Servicios - 20 -
2.1.4. Switching en un entorno LAN y WAN - 20 -
2.2. Simulador GNS3 - 22 -
2.2.1. Introducción a GNS3 - 22 -
2.2.2. Características de GNS3 - 23 -
2.2.3. Situación Actual de GNS3 - 23 -
2.2.4. Escenarios de GNS3 - 24 -
2.3. Dynagen/Dynamips - 25 -
2.3.1. Introducción - 25 -
2.3.2. Situación Actual - 26 -
2.3.3. Características de Dynamips - 26 -
2.3.4. Escenarios de Dynamips - 26 -
2.3.5. Imágenes IOS - 28 -
2.3.6. Utilización de Recursos - 29 -
2.3.7. Ejemplo de una topología básica - 30 -
2.3.8. Comunicación con las redes reales - 31 -
2.4. Herramienta para analizar tráfico de paquetes IP - 31 -
2.4.1. Wireshark - 31 -
2.4.2. Interfaz de Usuario - 32 -
2.5. Alcances y Limitaciones - 34 -

CAPÍTULO 3 ..... - 35 -
TECNOLOGÍAS QUE SE PUEDEN SIMULAR CON GNS3 ..... - 35 -
3.1. Frame Relay - 35 -
3.1.1. La Era Frame Relay - 36 -
3.1.2. Servicios - 36 -
3.1.3. Interoperatividad Frame Relay / ATM - 37 -
3.2. MPLS (Multiprotocol Label Switching) - 38 -
3.2.1. Antecedentes de MPLS - 38 -
3.2.2. Definición General de MPLS - 39 -
3.2.2.1. Ventajas de MPLS frente a tecnologías anteriores - 39 -
3.2.2.2. Características - 40 -
3.2.3. Elementos Básicos de Mpls - 41 -
3.2.3.1. Label Edge Router (LER) - 41 -
3.2.3.2. Label Switching Router (LSR) - 42 -
3.2.3.3. Forward Equivalence Class (FEC) - 42 -
3.2.3.4. Label Distribution Protocol (LDP) - 43 -
3.2.3.5. Label Switched Path (LSP) - 44 -
3.2.3.6. Label Information Base (LIB) - 44 -
3.2.4. Encabezado de Mpls - 45 -
3.2.5. Descripción Funcional de Mpls - 46 -
3.2.5.1. Funcionamiento del Plano de Control - 46 -
3.2.5.2. Funcionamiento del Plano de Envío - 47 -
3.2.6. Aplicaciones de MPLS - 48 -
3.2.6.1. Ingeniería de Tráfico - 48 -
3.2.6.2. Calidad de Servicio - 49 -
3.3. VPN (Virtual Private Network) - 49 -
3.3.1. Ventajas y desventajas de las VPN’s - 50 -
3.3.2. Generalidades de la Arquitectura de las VPN/MPLS. - 51 -
3.3.2.1. Route Distinguisher - 51 -
3.3.2.2. Route Target - 51 -
3.4. VPLS (Virtual Private LAN Service) - 52 -
3.4.1. Descripción - 52 -
3.4.2. Elementos de Red - 54 -
3.5. VLAN’S (Virtual LAN) - 55 -
3.5.1. Concepto de VLAN - 55 -

3.5.2. Ventajas de las VLAN - 55 -
CAPÍTULO 4 ..... - 58 -
DISEÑO METODOLÓGICO PARA INTEGRACIÓN DE LA CÁTEDRA LABORATORIO DE TELEMÁTICA..... - 58 -
4.1. Formulación de un pensum en la cual se integra la cátedra Laboratorio de Telemática. - 58 -
4.1.1. Número de Horas y Créditos al aprobar Laboratorio de Telemática. - 58 -
4.1.2. Vista del pensum académico actual. - 59 -
4.1.3. Vista del nuevo pensum académico. - 63 -
4.2. Planificación del calendario académico para la cátedra Laboratorio de Telemática. - 68 -
4.2.1. Ponderación del puntaje correspondiente a la materia Laboratorio de Telemática. - 68 -
4.2.2. Calendario de actividades de la materia Laboratorio de Telemática. - 69 -
4.3. Diseño de los escenarios de las prácticas de laboratorio de acuerdo a la planificación de la materia.- 69 -
4.3.1. Escenario 1: Conexión de 3 routers Cisco con GNS3 - 70 -
4.3.2. Escenario 2: Conexión de equipos reales con GNS3 - 72 -
4.3.3. Escenario 3: Conectividad entre routers reales y simulados - 74 -
4.3.4. Escenario 4: Interacción entre diferentes VM - 75 -
4.3.5. Escenario 5: Conexión con 802.1Q - 76 -
4.3.6. Escenario 6: Creación de VPN - 80 -
4.3.7. Escenario 7: Simulación de Acceso remoto - 86 -
4.3.8. Escenario 8: Creación VLAN de Gestión - 88 -
CAPÍTULO 5 ..... - 94 -
PRESUPUESTO APROXIMADO DEL COSTO PARA INTEGRACION DE LA MATERIA LABORATORIO DE TELEMATICA ..... - 94 -
CAPÍTULO 6 ..... - 96 -
CONCLUSIONES Y FUTUROS TRABAJOS..... - 96 -
1.1 Conclusiones - 96 -
1.2 Futuros Trabajos - 97 -
REFERENCIAS BIBLIOGRAFICAS..... - 98 -
ANEXOS..... - 100 -

ÍNDICE DE FIGURAS

CAPÍTULO 2

Figura 2.1 - Laboratorio de Telemática Universidad de Jaén 18
Figura 2.2 - Esquema de una Red en un entorno LAN y WAN 19
Figura 2.3 - Esquema de una red metro Ethernet de un ISP 20
Figura 2.4 - Conexión de sitios remotos en un entorno LAN 23
Figura 2.5 - Interconexión de dispositivos en entorno LAN y WAN 21
por medio de Switch 21
Figura 2.6 - Logotipo del Programa Simulad or 22
Figura 2.7 - Ejemplo de cableado y tipos 24
Figura 2.8 - Configuración básica de Dynagen/Dynamips 27
Figura 2.9 - Ejemplo de consola Dynagen 28
Figura 2.10 - Equipos soportados por el simulador 29
Figura 2.11 - Topología de conexión WAN punto a punto 30
Figura 2.12 - Esquema de conexión WAN punto a punto en el Simulador 30
Figura 2.13 - Conexión desde una NIC hacia redes reales 31
Figura 2.14 - Panel de paquetes IP capturados 33

CAPÍTULO 3

Figura 3.1 - Esquema de una conexión FrameRelay 35
Figura 3.2 - Modelo de FrameRelay sobre ATM 37
Figura 3.3 - Red básica MPLS 41
Figura 3.4 - FEC sin Agregación y con Agregación 43
Figura 3.5 - Estructura genérica de la cabecera MPLS 45
Figura 3.6 - Intercambio de Etiquetas de un dominio MPLS 47
Figura 3.7 - Arquitectura general de una red VPN/MPLS 52
Figura 3.8 - Esquema de una conexión VPLS 54
Figura 3.9 – Creación de VLAN 56

CAPÍTULO 4

Figura 4.1 - Red de 3 routers Cisco en GNS3 70
Figura 4.2 - Opciones de los routers en GNS3 71
Figura 4.3 - Creación de Interfaces 72
Figura 4.4 - Escenario a realizar por GNS3 73

Figura 4.5 - Asignación de Tarjetas de Red 73
Figura 4.6 - Red creada en GNS3 74
Figura 4.7 - Escenario completo de la red diseñada 74
Figura 4.8 - Realización de Ping desde PC2 a PC1 75
Figura 4.9 - Conexión con WebServer 76
Figura 4.10 – Escenario alternativo con otro router Cisco “PE” 76
Figura 4.11 –VLAN .1Q “506” 77
Figura 4.12 –Interfaz etiquetada .1Q 506 en GNS3 78
Figura 4.13 –Ping desde PC6 a PC7 79
Figura 4.14 –Conexión en el Switch 79
Figura 4.15 –Escenario para crear VPN 81
Figura 4.16 –Escenario creado en la VM1 82
Figura 4.17 –Escenario creado en la VM2 82
Figura 4.18 – Resultado de Ping y Traceroute desde el PC3 al PC5 83
Figura 4.19 –Resultado de Ping y Traceroute desde el PC3 al PC7 83
Figura 4.20 –Resultado de Ping desde el PC3 al PC4 84
Figura 4.21 –Resultado de Ping desde el PC3 al PC6 84
Figura 4.22 –Ping de PC4 a PC3 85
Figura 4.23 –Ping de PC4 a PC5 85
Figura 4.24 –Ping de PC4 a PC6 85
Figura 4.25 –Captura de la interfaz f1/0 entre PE1 y P (VM2) 86
Figura 4.26 –Escenario de conexión remota 87
Figura 4.27 –Ping de PC remoto a PC5 88
Figura 4.28 – Creación de VLAN de Gestión 89
Figura 4.29 –Escenario VLAN de gestión en GNS3 89
Figura 4.30 –Escenario completo VLAN de gestión 90
Figura 4.31 –Creación de VLAN con GNS3 91
Figura 4.32 –Conexión remota al router P 92
Figura 4.33 –Conexión remota al router PE1 92
Figura 4.34 –Conexión remota al router PE2 92

ÍNDICE DE TABLAS

CAPÍTULO 3

Tabla 3.1 - Ejemplo de la información proporcionada por una tabla LIB 45

CAPÍTULO 4

Tabla 4.1 - Asignaturas correspondientes al I CICLO actual 59
Tabla 4.2 - Asignaturas correspondientes al II CICLO actual 59
Tabla 4.3 - Asignaturas correspondientes al III CICLO actual 60
Tabla 4.4 - Asignaturas correspondientes al IV CICLO actual 60
Tabla 4.5 - Asignaturas correspondientes al V CICLO actual 61
Tabla 4.6 - Asignaturas correspondientes al VI CICLO actual 61
Tabla 4.7 - Asignaturas correspondientes al VII CICLO actual 62
Tabla 4.8 - Asignaturas correspondientes al VIII CICLOactual 62
Tabla 4.9 - Asignaturas correspondientes al IX CICLO actual 63
Tabla 4.10 - Asignaturas correspondientes al I CICLOnuevo 63
Tabla 4.11 - Asignaturas correspondientes al II CICLO nuevo 64
Tabla 4.12 - Asignaturas correspondientes al III CICLO nuevo 64
Tabla 4.13 - Asignaturas correspondientes al IV CICLO nuevo 65
Tabla 4.14 - Asignaturas correspondientes al V CICLO nuevo 65
Tabla 4.15 - Asignaturas correspondientes al VI CICLOnuevo 66
Tabla 4.16 - Asignaturas correspondientes al VII CICLO nuevo 66
Tabla 4.17 - Asignaturas correspondientes al VIII CICLOdonde se integrará la materia Laboratorio de Telemática 67
Tabla 4.18 - Asignaturas correspondientes al IX CICLO nuevo 67
Tabla 4.19 - Calendario de actividades de la materia Laboratorio de Telemática durante un semestre regular 69

CAPÍTULO 5

Tabla 5.1 - Coste del Software 80
Tabla 5.2 - Coste de equipos físicos 80
Tabla 5.3 - Coste total del proyecto 81

CAPÍTULO 1
DISEÑO DEL TRABAJO DE TITULACIÓN

1.1. Introducción

El presente trabajo de graduación es la propuesta de la integración de la materia Laboratorio de Telemática para la Facultad Técnica, conociendo que dentro del pensum académico existen las materias Telemática 1 y 2, pero que a la vez estas no se complementan con prácticas de escenarios basados en topologías de redes IP reales, debido a esto nos basaremos en un simulador de gran calidad como lo es el GNS3 y así poder realizar la virtualización de estos equipos de comunicaciones y pulir los conocimientos obtenidos en las materias teóricas.

Las Telecomunicaciones hoy en día han evolucionado hasta llegar a la gran convergencia tecnológica llamada IP, el transporte de los datos e información ya no se limita a ser realizada por equipos SDH y DWDM, sino que ahora se lo puede lograr de una forma más versátil y flexible por medio de equipamiento que hablan el protocolo internet. El Protocolo Internet se ha estandarizado y puede ser soportado e interactuar en cualquier equipamiento o fabricante. Los profesionales deben estar preparados para poder asumir el gran reto de administrar, configurar y comisionar los equipos IP en entornos LAN y WAN.

Las RedesIP en un entorno ISP cuentan con diversidad de tecnologías de transporte y acceso y se compone de diferentes fabricantes pero el concepto y los principios son los mismos, los fabricantes de dispositivos cambian el entorno grafico o líneas de comandos, pero en esencia los modos de configuración son iguales.

Las redes de datos actuales a nivel de transporte se realizan mediante un dispositivo de red IP llamado router, el cual puede tener una gran capacidad de procesamiento y puede soportar diversidad de tecnologías, que por medio del simulador se analizaran en la materia que integraremos.

1.2. Justificación

Actualmente se ha generado una competencia en el mercado de las telecomunicaciones por contratar ingenieros que posean sólidos conocimientos de redes y direccionamiento IP, ya que los servicios que antes se brindaban de forma separada como la telefonía, la gestión remota e internet se pueden brindar sobre una infraestructura de red compartida como lo es una red IP.

Los estudiantes que salen de las universidades a nivel general carecen o tienen muy poco conocimiento de cómo enfrentar los retos como el networking y tecnologías IP a nivel de entornos LAN y WAN, y lo que se hace hoy en día tradicionalmente es tomar cursos CISCO para nivelar sus falencias o conocimientos relativos a la materia de Telemática, y es causado por no tener una combinación de fundamentos de redes IP, más practicas en laboratorios con casos reales de configuración de un escenario. La mejor forma de vencer estos inconvenientes, es integrando una cátedra en la que se puede contar con un pensum y con un simulador que este en capacidad de soportar la mayoría de las tecnologías IP actuales como si se estuviera frente a la consola de un dispositivo real, los equipamientos para poder realizar prácticas de direccionamiento IP son muy costosos y están fuera del alcance de un presupuesto. En la facultad se cuenta con diversidad de materias de telecomunicaciones, dentro de las cuales TELEMATICA 1 y 2, brindan las directrices para empezar en el mundo IP, pero no se está solidificando la teoría con la práctica.

La facultad técnica para el desarrollo al integrar la cátedra de Laboratorio de Telemática con el pensum que se propondrá y con la ayuda del simulador para poner en práctica los conocimientos adquiridos formará ingenieros que estarán en capacidad de salir a trabajar en áreas afines como administrador de redes, ingeniería junior de voz y datos, ingenieros de soporte o se pondrán desempeñar en entornos de ServicesProviders.

1.3. Planteamiento del Problema

Debido a la falta de prácticas a nivel de redes IP se plantea integrar a la facultad técnica para el desarrollo, una cátedra que interactuará con un potente simulador que permite cargar IOS verdaderos de routers y switches Cisco, además poder ejecutar comandos que no son soportados por ningún otro simulador, y así formar ingenieros con bases sólidas entorno al networking.

El pensum que se aplicara a la cátedra deberá ser cuidadosamente estructurado ya que debe ser una teoría aplicada a la práctica, se deberá contar con maquinas que corran Windows 7,donde se instalara el programa, se tendrá que contar con IOS verdaderos que ya se los debe obtener con sus respectivas licencias desde la pagina de Cisco.

Se empezará con una introducción básicahasta llegar a configurar entornos para expertos de nivel 3.

Nuestra oferta se planteara en cinco pasos expuestos a continuación:

1) Pensum de la Cátedra Laboratorio de Telemática.
2) Adquisición del simulador de redes IP GNS3.
3) Adquisición de las IOS de routers y switches Cisco.
4) Topologías de configuración en base al pensum.
5) Casos Prácticos aplicadoa ISP y entorno LAN.

En lo que respecta a los casos prácticos hacemos referencia a la realización de cada escenario de acuerdo al pensum que hemos de realizar y así algún otro grupo de la Facultad Técnica pueda pulir nuestro trabajo realizando la implementación de cada uno de los escenarios planteados aquí.

1.4. Objetivo General

Integrar la cátedra de Laboratorio de Telemática en la Facultad Técnica para el Desarrollo por medio de un simulador para optimizar y formar ingenieros que posean sólidos conocimientos de direccionamiento IP y poder aplicarlos en Carriers y empresas que brinden soluciones IP.

1.5. Objetivos Específicos

- Integrar la cátedra de Laboratorio de Telemática diseñando un pensum que permita aplicar lo aprendido en un simulador real.
- Utilizar una plataforma de simulación para redes reales y tecnologías IP de última generación.
- Diseñar soluciones para ISP(Internet ServiceProviders) y networking de nivel 2 y 3
- Formar ingenieros que posean sólidos conocimientos a nivel del networking, ya que el mercado de las telecomunicaciones hoy en día exige de profesionales certificados en Cisco o con amplios conocimientos de networking, es ahí donde los nuevos ingenieros podrán demostrar lo que aprenderán del Laboratorio de Telemática.

1.6. Hipótesis

La integración de la cátedraLaboratorio de Telemáticaayudará a que los estudiantes puedan aplicar los conocimientos adquiridos en las materias de Telemática 1 y 2; y a su vez estar en capacidad de poner a prueba sus conocimientos obtenidos mediante esta materia en empresas líder en el mercado de las telecomunicaciones, y así no solo formar ingenieros de campo, sino también profesionales que se dediquen a dar soluciones de Networking, sin necesidad de tener una certificación adicional.

1.7. Metodología de Investigación

Para la integración de la cátedra Laboratorio de Telemática usaremos el método científico. Cabe recalcar que cada uno de los escenarios para las prácticas del nuevo laboratorio de telemática es sumamente investigativo, con lo cual se puede partir para la implementación final de este proyecto, para aquello otro grupo interesado deberá enfocarse totalmente en la planificación, implementación y demás detalles de cada una de las prácticas del nuevo laboratorio de telemática partiendo desde los escenarios ya creados en nuestra investigación.

CAPÍTULO 2
FUNDAMENTOS TEORICOS

2.1. Laboratorio de Telemática

En este capítulo se realizara una fundamentación teórica sobre lo que concierne a nuestra materia Laboratorio de Telemática, y a su vez se explicará la forma de uso del simulador de redes GNS3.

2.1.1. Introducción

Los laboratorios de redes IP hoy en día son los pilares para cimentar los conocimientos de los estudiantes de tecnologías IP, se pueden encontrar en ellos equipamientos altamente sofisticados desde un router 1700 hasta un router 7600 o GSR 1200 que se escapa de los presupuestos de las academias tecnológicas, motivo por el cual se ha implementado y popularizado el uso de simuladores para suplir estas falencias, el Laboratorio de Telemática será virtual pero se podrá disponer de equipos que poseen las últimas tecnologías IP como Routers de la serie Cisco 7200, 3800, switches,FrameRelay, Switch de capa 2 y 3, etc., se pretende que el estudiante aprenda a configurar routers y switches principalmente ya que la mayoría de los servicios hoy en día se basan en Routing y Switching de capa 2 y 3.

A continuación se muestra una perspectiva de a donde se quiere llegar con la integración de esta cátedra de Laboratorio de Telemática para la Facultad Técnica.

Figura 2.1 – Laboratorio de TelemáticaUniversidad de Jaén

Fuente: http://www10.ujaen.es/node/10550

2.1.2. El uso de dispositivos IP en ISP's y redes locales

Las redes IP actuales cuentan con dispositivos de red altamente sofisticados para el transporte de datos entre los cuales sobresalen los routers y switches de capa 2 y 3.

Los ISP (Internet ServicesProviders) cuentan con diversidad de tecnologías sobre equipos como routers que son los encargados de transportar el tráfico de IP desde un origen hasta un destino, pero sobre él se pueden montar diversidad de protocolos y tecnologías dependiendo de la necesidad del ISP,estos dispositivos son administrables y se necesita tener un grado de conocimientos intermedio para poder realizar mantenimientos y configuración de los mismos, un ISP puede tener routers interactuando entre sí de distintos fabricantes, como Cisco, Huawei, Tellabs, etc.Pero la teoría es la misma solo cambian los entornos gráficos y de comandos, pero se ha estandarizado el manejo de equipamiento cisco ya que es el pionero en este tipo de servicios.

A continuación se puede visualizar un ejemplo de un entorno de red WAN y LAN con equipamiento de red que se puede simular.

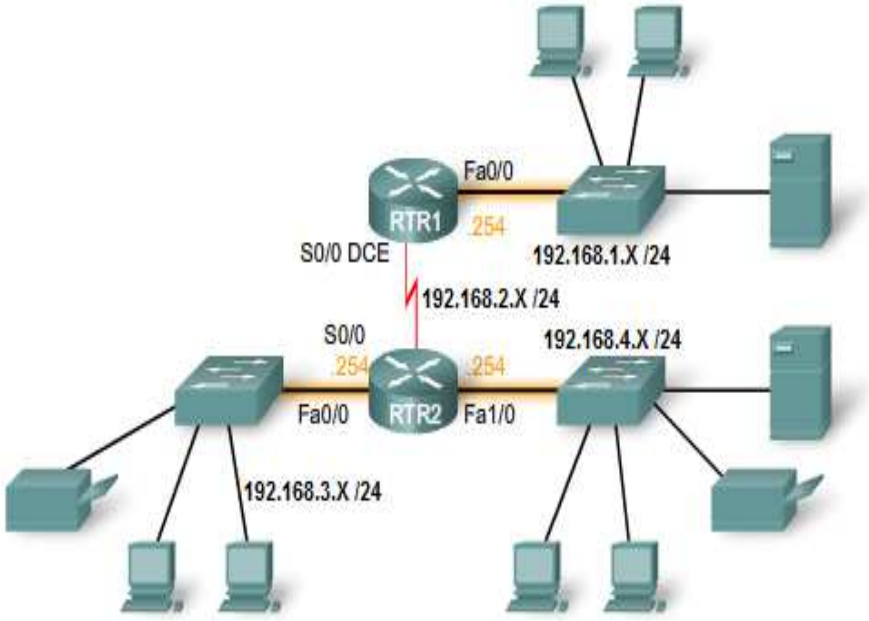


Figura 2.2 – Esquema de una Red en un entorno LAN y WAN

Fuente: (CISCO 1, Networking Academy, 2010)

2.1.3. Routing en un entorno de Proveedor de Servicios

En un proveedor de Servicios de Internet, el equipamiento que sobresale es el dispositivo llamado Router, que es el encargado de transportar el tráfico IP desde un punto de origen hasta un destino sin importar el medio de transmisión pudiendo ser este cobre, RF o fibra, dependiendo de las velocidades y acceso de las interfaces.

Los Routers en entornos ISP a nivel de transporte ya se encuentran en capacidad de transportar paquetes IP en el orden de las ten gigas, con lo cual se puede tener una capacidad de transporte ilimitada. El Routing se basa en protocolos de enrutamiento que son algoritmos que se encargan de elegir la mejor ruta para optimizar el tiempo en envío de losdatos, estos protocolos están estandarizados para poder trabajar con cualquier fabricante, con lo cual se puede tener una red híbrida a nivel de fabricantes pero unificada a nivel de tecnología.(CISCO 2, Networking Academy, 2009)

A continuación se puede apreciar un esquema de routers en un entorno metro Ethernet interactuando con Dslam de acceso.

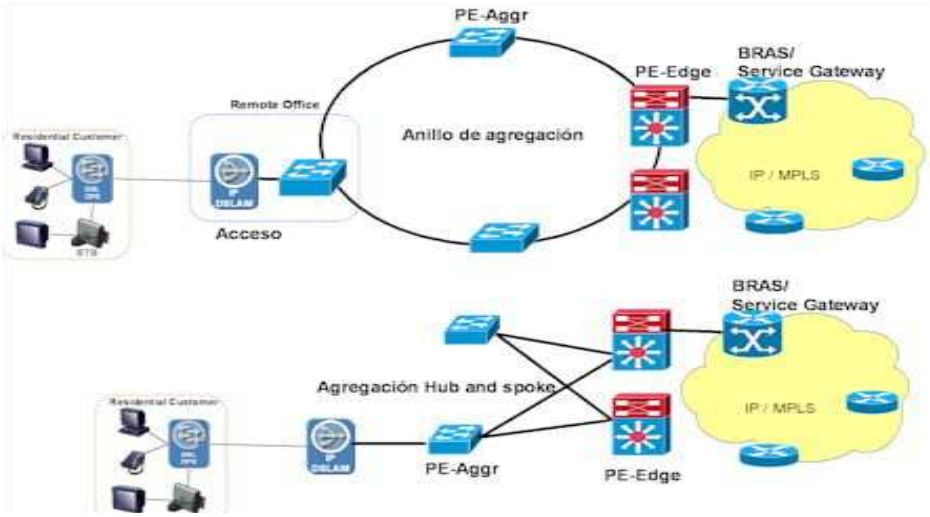


Figura 2.3 – Esquema de una red metro Ethernet de un ISP

Fuente: http://www.oas.org/en/citel/infocitel/2007/enero/multiservicio_e.asp

2.1.4. Switching en un entorno LAN y WAN

El Switching como su palabra lo indica nos ayudará en la conmutación del tráfico de paquetes para un servicio apropiado y aparte nos ayuda a segmentar una red en dominios de difusión para optimizar los recursos de procesamiento y tratamiento de los paquetes IP.

El Switching es una técnica que fue creada para entorno LAN, para poder conectar dispositivos de red como PC's, cámaras IP, servidores, impresoras, etc.

Existen dos tipos de Switching, el primero se lo conoce como Switching de capa 2 y se basa en el envío de los datos tomando en cuenta solo la dirección Mac de los dispositivos de red, mientras que el segundo llamado Switching de capa 3 el envío se basa en la dirección Mac o física y la dirección IP de capa 3, lo cual lo hace más robusto pero el costo del mismo es superior al de la capa 2.

En la siguiente figura se puede apreciar la técnica de Switching para poder interconectar 3 sitios remotos como si estuvieran en un mismo dominio de colisión o conectados a un mismo switch.(David Luna, 2005)

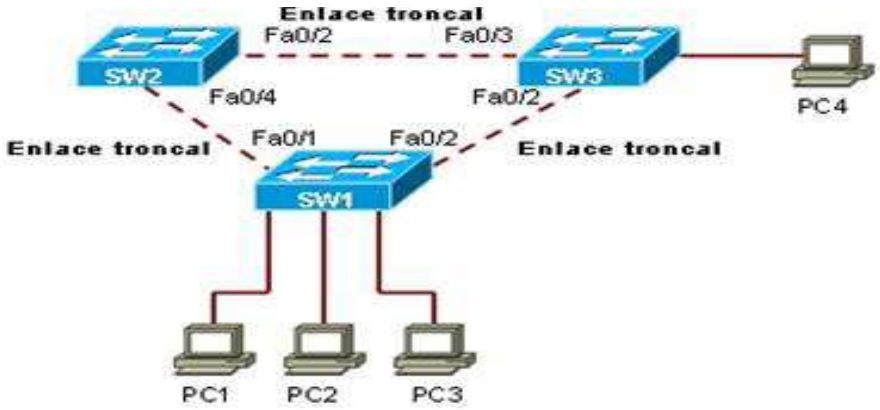


Figura 2.4 – Conexión de sitios remotos en un entorno LAN

Fuente: http://es.scribd.com/doc/12487509/Cisco-CCNA-2-Exploration

En la siguiente figura se puede apreciar el Switching en un entorno LAN.

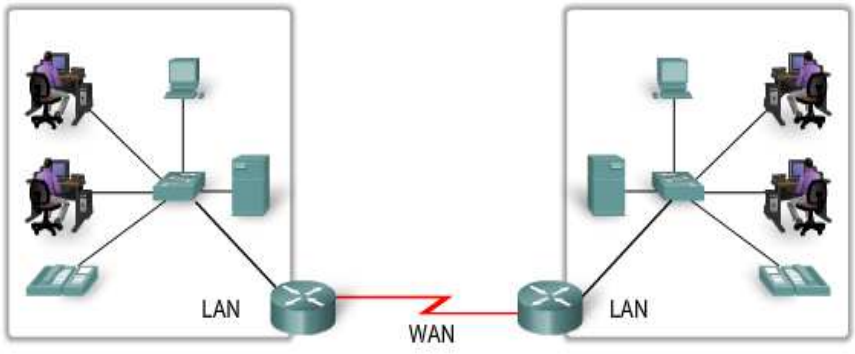


Figura 2.5 – Interconexión de dispositivos en entorno LAN y WAN por medio de Switch

Fuente: (CISCO 1, Networking Academy, 2010)

2.2. Simulador GNS3

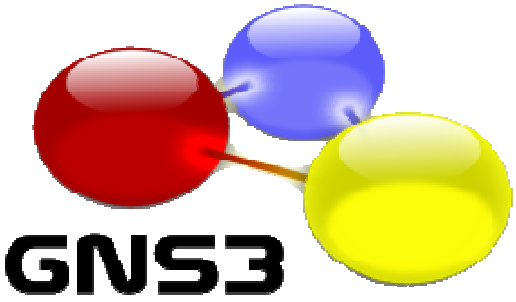


Figura 2.6 – Logotipo del Programa Simulador

Fuente: http://ebookee.org/GNS3-Tutorials-For-CCNA-CCNP-CCIE-Candidates-With-GNS3-Live-CD_1338164.html

2.2.1. Introducción a GNS3

GNS3 es un simulador gráfico de redes que le permitirá diseñar fácilmente topologías de red y luego ejecutar simulaciones en él, éste utiliza las aplicaciones:

- **Dynamips,** el núcleo del programa que permite emulación las imágenes *IOS* de Cisco.
- **Dynagen,** un texto basado en *front-end*para Dynamips.
- **Pemu**, un servidor de seguridad PIX de Cisco, para salvar las configuraciones.
- **Wireshark**, un capturador de paquetes.

GNS3 es una herramienta complementaria para los laboratorios de redes de Ciscopara ingenieros, administradores y personas que quieran pasar las certificaciones
CCNA, CCNP, CCIE o DAC.(GNS3 Graphical Network Simulator, 2007)
Es un proyecto de código abierto, programa libre que puede utilizarse en múltiplessistemas operativos, como: Windows, Linux y Mac.
Hasta este momento GNS3 soporta el IOS de routers, ATM/FrameRelay/Switchs Ethernet y Pix Firewalls.
Usted puede extender su red propia, conectándola a la topología virtual por medio de una conexión virtual entre su tarjeta de red y una red real.
Para realizar esta magia, GNS3 está basado en Dynamips, PEMU **(**incluyendo el encapsulador) y en parte en Dynagen, fue desarrollado en python a través de PyQt la

interfaz grafica (GUI) confeccionada con la poderosa librería Qt, famosa por su uso en el proyecto KDE.

GNS3 también utiliza la tecnología SVG (Scalable Vector Graphics) para proveer símbolos de alta calidad para el diseño de las topologías de red.

2.2.2. Características de GNS3

Sus principales características se pueden resumir en los siguientes puntos:

- Dispone de una interfaz gráfica de alta calidad con la que se pueden diseñar complejas topologías de red.
- Puede emular una gran cantidad de plataformas de *router*Cisco y firewall, así como la creación de diferentes elementos necesarios como son PCs, conmutadores, hub, etc.
- También puede simular un gran número de interfaces como Ethernet, ATM, FrameRelay, destacando lo simple que es su manejo.
- Contará con conexiones de red con las que se podrán simular redes del mundo real, además de poder conectarse a ellas.
- Utiliza el programa Wireshark para capturar los paquetes de red.

Hay que tener en cuenta que las imágenes IOS las tienen que aportar el administrador de la herramienta, ya que no es de libre distribución y tiene que ser Cisco quien la suministre para poder usarla en la aplicación GNS3, igual que ocurre si se desea utilizar Dynagen/Dynamips.(Segundo, 2009)

2.2.3. Situación Actual de GNS3

GNS3 está destinado a complementar la aplicación Dynamips para que al usuario lesea más fácil la instalación, la creación de escenarios y su visualización.

Cuando se instala GNS3 se puede observar que las herramientas antes mencionadas(Dynagen, Dynamips y Pemu) quedan instaladas y configuradas. Sólo hará falta laconfiguración de la imagen IOS, además de su ubicación, para guardar los futurosescenarios.(GNS3 Graphical Network Simulator, 2007)

A la hora de crear los escenarios con GNS3 va a resultar más sencillo, ya que sólohabrá que arrastrar los *routers*que se quieran utilizar e ir cableándolos. Esta manera detrabajar facilitará la conexión entre redes, debido a que tiene instalado un software quepermite la configuración de todas las tarjetas Ethernet que se tengan instaladas. Estopermite hacer tantas configuraciones como se desee, ya sean virtuales como reales.

GNS3 facilita los siguientes modos de funcionamiento:

- La construcción de la topología.
- La ejecución y parada de órdenes en las máquinas simuladas.
- La destrucción de la topología.
- La conexión con redes existentes mediante tarjetas Ethernet.
- La posibilidad de salvar configuraciones, tanto de los *routers*como del propioescenario.
- Los distintos paquetes que se pueden analizar mediante el programa Wireshark utilizando diferentes protocolos.

2.2.4. Escenarios de GNS3

El escenario más sencillo que se puede construir es la simulación entre un par de*routers*. El cableado utilizado podrá ser variado y se podrán realizar interfaces Ethernet,Serial, ATM, etc., para lo cual lo único que se tiene que hacer es ir conectándolos, comose puede ver en el ejemplo (Figura 2.7).

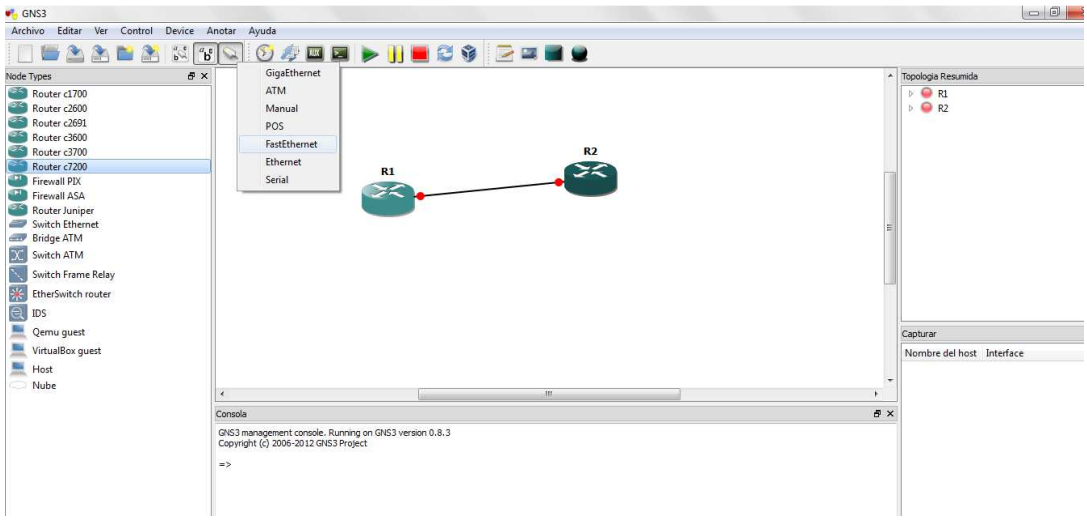


Figura 2.7 - Ejemplo de cableado y tipos

Fuente:los autores

Una vez diseñado el escenario, sólo se tendrán que iniciar los *routers*y activar laconsola. Tras su inicialización se estará en disposición de configurar los *routers*desdecero, como si fuesen *routers*reales.

2.3. Dynagen/Dynamips

2.3.1. Introducción

Dynagen, también conocido como Dynamips, es un *front-end*o lo que es lo mismo, estado inicial de un proceso, para la emulación de escenarios de red. Por tanto Dynamips, es un emulador de *router*Ciscos.

Emula las plataformas hardware: 1700, 2600, 3600, 3700, 7200 y ejecuta imágenes *IOS5* estándar.

El emulador no reemplaza a *routers*reales, es una herramienta complementaria muy útil para laboratorios o usuarios que quieran pasar los certificados Cisco CCNA /CCNP / CCIE. Utiliza un simple archivo de configuración XML, (al igual que VNUML), y especifica configuraciones hardware para *routers*virtuales.

El verdadero potencial de este simulador se encuentra en que emula directamente la imagen IOS del *router*. Está escrito en *Python6* y su diseño es modular. También cuenta con una aplicación gráfica GNS3 muy intuitiva y fácil de manejar, similar a BOSON.

Dynamips es un emulador de routers Cisco escrito por ChristopherFillot. Emula a las plataformas 1700, 2600, 3600, 3700 y 7200, Firewall Pix, Switching, ASA y ejecuta imágenes de IOS estándar.(Anuzelli)

Este tipo de emulador será útil para:

- Ser utilizado como plataforma de entrenamiento, utilizando software del mundo real. Permitirá a la gente familiarizarse con dispositivos Cisco, siendo Ciscoel líder mundial en tecnologías de redes.
- Probar y experimentar las funciones del Cisco IOS.
- Verificar configuraciones rápidamente que serán implementadas en routers reales.
- Por supuesto, este emulador no puede reemplazar a un router real, pero es una herramienta complementaria para los administradores de redes o para aquellos que desean optimizar sus conocimientos en redes IP.

2.3.2. Situación Actual

Dynagen está destinado a la aplicación de redes y servicios en modo de prueba, yaque permite la ejecución de *routers*Cisco del mismo modo que se realiza en la realidadcon varios nodos. Esta aplicación no necesita de una gran inversión ni la complejidad dela gestión necesaria para crear equipos reales.

Dynagen facilita la conexión entre diferentes redes ya que consta de tantasinterfaces como sean necesarias para conectarse con el exterior.

Dynagen soporta los siguientes modos de funcionamiento:

- Construcción de la topología de la simulación.
- Ejecución y parada de órdenes en las máquinas simuladas.
- Destrucción de la topología.
- Creación interfaces con el exterior.

2.3.3. Características de Dynamips

Dynamips utiliza una buena cantidad de memoria y CPU a fin de lograr su emulación, por lo que asigna todos sus recursos. Por esto es necesaria una máquina exclusivamente para su uso. Cuanto mayor es el número de *routers*a emular, mayor capacidad de recursos se consumirá. Dynamips asigna por defecto 16 MB de RAM en sistemas Windows y 64MB en sistemas Unix. Esto se debe a que por defecto Dynamips usa archivos mapeados en memoria para el direccionamiento en la memoria virtual.

La única manera de utilizar menos memoria es ajustándolo manualmente en el dispositivo o *router*. El motivo de que utilice tanta CPU, es porque se trata de una emulación de la CPU del *router*instrucción por instrucción. Debido a que inicialmente no sabe cuando el *router*virtual está inactivo, constantemente está ejecutando las instrucciones que componen la imagen IOS y las rutinas de ejecución de instrucciones que realizan. Pero una vez que ha ejecutado las imágenes IOS, la utilización de la CPU disminuye.(GNS3 Graphical Network Simulator, 2007)

2.3.4. Escenarios de Dynamips

Para generar los escenarios, primero se necesitará saber la metodología de trabajo,por tanto, se describirá el procedimiento a seguir. Se empezará escribiendo la

máquinadonde se va a ejecutar la aplicación Dynagen/Dynamips, para lo cual se pondrá:**[localhost]**. Por el contrario, si no es la misma máquina se tendrá que poner el nombre*host* o la dirección IP de la máquina donde se vaya a ejecutar.

La siguiente instrucción que se escribirá será el *router*Cisco a utilizar, en esteejemplo se pondrá: **[[7200]]**, hay que fijarse que este irá entre doble corchetes.

Después se tendrá que poner la imagen IOS con su ubicación en el sistema, porejemplo: **imagen=c7200-jk903-mz-7a.image** y se indicarán sus características: **NPE =NPE-400** y **RAM= 160** asignada en MB.

Una vez especificadas las características se crearán los *routers*que van a ser usados,estos también tendrán que ir entre doble corchetes **[[Router R1]]**. Se le irán asignandolas interfaces correspondientes como se indica en el ejemplo: **s1/0 = R2 s1/0**. En esteejemplo se especifica una interfaz serial 1/0 que se conecta con el *router*R2, donde éstetambién utilizará la interfaz serial 1/0.

Dynagen puede capturar los paquetes tanto en las interfaces virtuales Ethernet como Serial, utilizando la aplicación Wireshark.

Al igual que se indicó en GNS3, el escenario más simple será crear un escenariocon un par de *routers*. En este caso el configurarlo se hace más costoso, ya que primerohay que crear un fichero de texto, escribir la configuración (Figura 2.8) y cambiarle la extensión para que lo reconozca la aplicación Dynagen.(Anuzelli)

```
[localhost]

    [[7200]]
    image = \Program Files\Dynamips\images\c7200-jk9o3s-mz.124-7a.image
    # On Linux / Unix use forward slashes:
    # image = /opt/7200-images/c7200-jk9o3s-mz.124-7a.image
    npe = npe-400
    ram = 160

    [[ROUTER R1]]
    s1/0 = R2 s1/0

    [[router R2]]
```

Figura 2.8 - Configuración básica de Dynagen/Dynamips

Fuente: http://es.scribd.com/doc/75286465/VlAN

Habrá que tener en cuenta que los *routers*tendrán que estar identificados (tener unnombre) para poder referirse a ellos a la hora de crear las interfaces, como se puedecomprobar en la Figura 2.8.

Una vez creado el escenario, ya se puede ejecutar el fichero, pero primero tendráque estar activo el servidor de Dynamips (*Dynamips Server*). Una vez cargado elservidor se podrá ejecutar el fichero ".net" generando la consola Dynagen. Desde estaconsola es desde donde se podrán realizar: la llamada a las consolas de los *routers*, lacaptura de los paquetes, así como poder guardar la configuración de los *router*; como sepuede comprobar en la Figura 2.9.

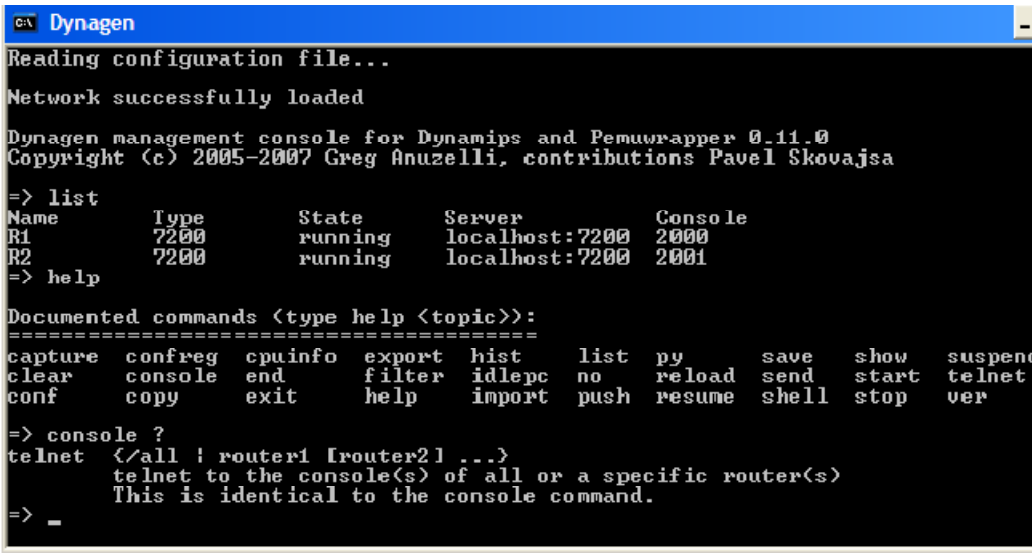


Figura 2.9 - Ejemplo de consola Dynagen

Fuente: http://es.scribd.com/doc/75286465/VlAN

Como se puede observar, todo este proceso es más engorroso y podría serconveniente utilizar la interfaz gráfica.

2.3.5. Imágenes IOS

Las imágenes IOS que son soportados en el simulador pueden emular cualquier tipo de tecnología IP, ya que las versiones son 12.4 y cuenta con toda la gama de protocolos y comandos que un router real, las imágenes necesitan descomprimirse cada vez se ejecuta un router en el simulador. Por tal motivo el programa permite realizar una operación que optimiza el uso en la capacidad del consumo de memoria calculando un valor diferente por cada modelo de router aplicada la imagen respectiva.

Las imágenes Cisco IOS están comprimidas. Estas imágenes comprimidas funcionan bien con Dynamips, aunque el proceso de arranque es significativamente más lento debido a la descompresión (igual que en los routers reales). Es recomendable

descomprimir las mismas de antemano así el emulador no tiene que realizar esa tarea. Las imágenes y tecnologías que soporta el simulador son:

C1700, C2600, C3600, C3700, C7200, PIX FIREWALL, ASA FIREWALL, ATM, FRAME RELAY, SWITCHING.(Anuzelli)

A continuación se puede apreciar las opciones que permite simular el programa:

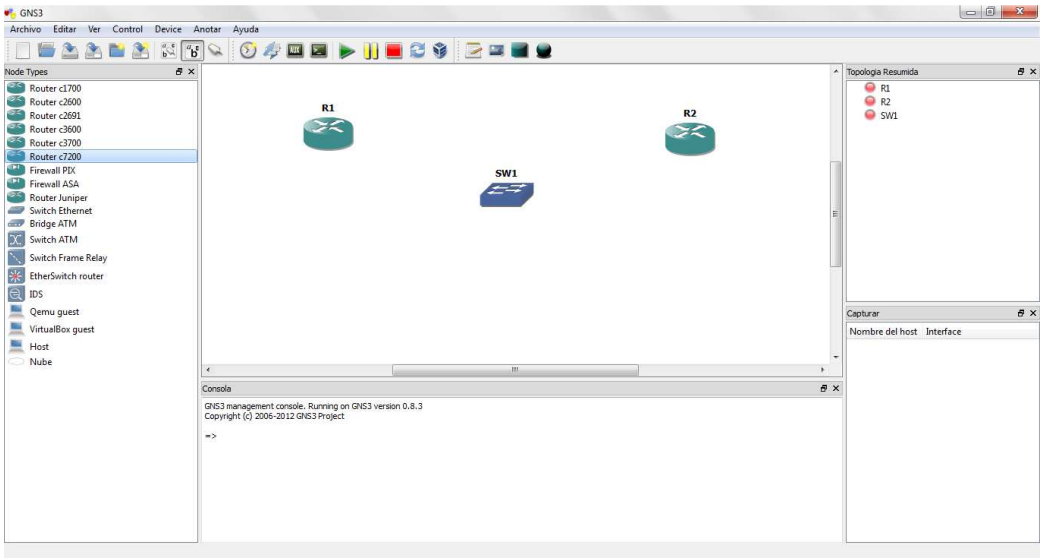


Figura 2.10 -Equipos soportados por el simulador

Fuente: los autores

2.3.6. Utilización de Recursos

Dynamips hace uso intensivo de memoria RAM y CPU en orden de lograr la magia de la emulación. Si su intención es de ejecutar una imagen de IOS que requiere 256MB de RAM en un router 7200 real, y dedica 256 MB de RAM a la distancia de su router virtual, este utilizará 256MB de memoria para funcionar.

Dynamips también hace uso intensivo de CPU, porque esta emulando la CPU de un router instrucción por-instrucción. En principio no tiene manera de saber cuando el router virtual está en estado ocioso (idle), por esa razón ejecuta diligentemente todas las instrucciones que conforman el “real “funcionamiento. Pero una vez que haya ejecutado el proceso de “Idle-PC” para una determinada imagen de IOS, la utilización de CPU decrecerá en forma drástica.

2.3.7. Ejemplo de una topología básica

A continuación se puede apreciar un escenario en un entorno LAN y WAN compuesto por 3 sitios remotos interconectados entre sí por medio de 3 routers cisco y estos a su vez se interconectan a la LAN por medio de un switch en donde a su vez se conectarán las estaciones de trabajo.

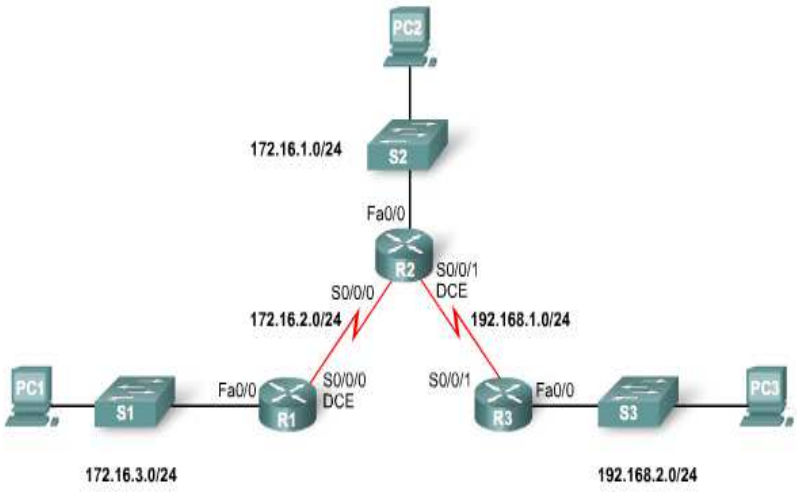


Figura 2.11–Topología de conexión WAN punto a punto

Fuente: (CISCO 1, Networking Academy, 2010)

En el simulador el escenario se vería de la siguiente manera:

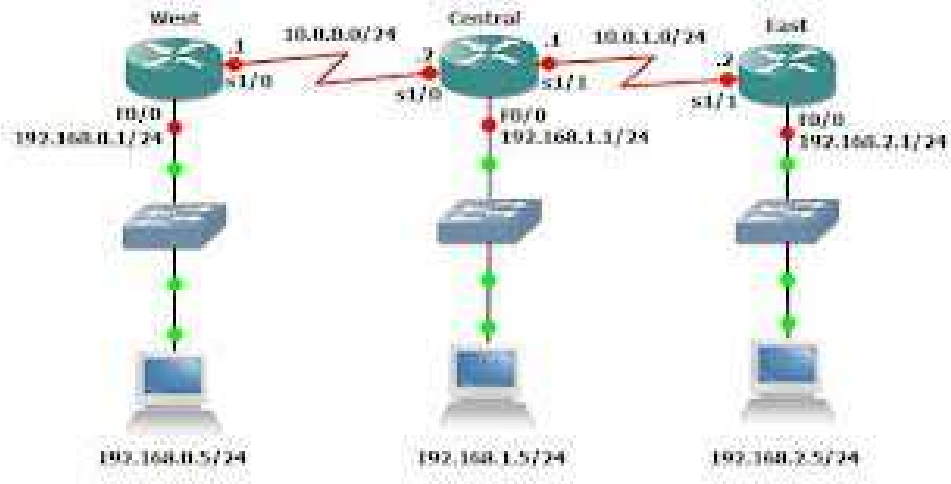


Figura 2.12 – Esquema de conexión WAN punto a punto en el Simulador

Fuente: los autores

2.3.8. Comunicación con las redes reales

Dynamips puede conectar las interfaces de los routers virtuales con interfaces reales de los hosts, posibilitando la comunicación entre su red virtual con el mundo real. Para hacer uso de esta función con GNS3, debe crear un dispositivo “NUBE”. Una Nube representa sus conexiones externas. A continuación debe configurarla. En este ejemplo adicionamos la NIO_gen_eth0.

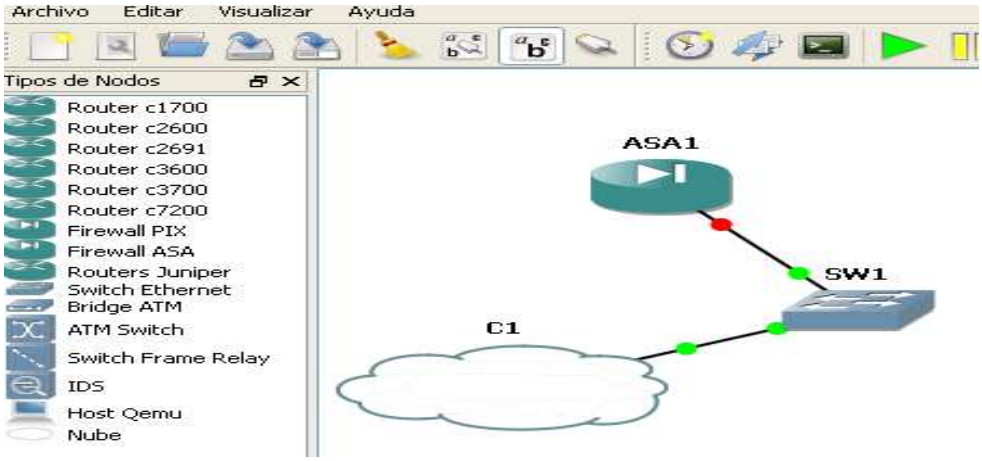


Figura 2.13 – Conexión desde una NIC hacia redes reales

Fuente: los autores

En el anterior ejemplo hemos conectado la interfaz del router e0/0 a la interfaz eth0 del host. Los paquetes que egresan de e0/0 son volcados en la red real a través de la interfaz eth0 del host, y los paquetes que regresan son encaminados de la misma manera a la instancia del router virtual.

2.4. Herramienta para analizar tráfico de paquetes IP

Hoy en día es muy importante poder realizar el análisis de trafico de paquetes IP, y esto es posible con una herramienta que permite capturar paquetes IP y ver el contenido del mismo llamado Wireshark.

2.4.1. Wireshark

Conocido como ETHEREAL es software de análisis de protocolos utilizada por los profesionales y/o administradores de la red para identificar y analizar el tipo tráfico en un momento determinado. En el argo IT se denominan analizadores de protocolos de red, analizadores de paquetes, *packetsniffer*o *sniffer*.

Ethereal permite analizar los paquetes de datos en una red activa como también desde un archivo de lectura previamente generado, un caso particular es generar un archivo con TCPDUMP y luego analizarlo con Ethereal.

Algunas de las características de WireShark son las siguientes:

- Disponible para UNIX, LINUX, Windows y Mac OS.
- Captura los paquetes directamente desde una interfaz de red.
- Permite obtener detalladamente la información del protocolo utilizado en el paquete capturado.
- Cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas.
- Filtra los paquetes que cumplan con un criterio definido previamente.
- Realiza la búsqueda de los paquetes que cumplan con un criterio definido previamente.
- Permite obtener estadísticas.
- Sus funciones gráficas son muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos.

Es importante tener presente que Wireshark no es un IDS (*InstrusionDetectionSystem*) ya que no es capaz de generar una alerta cuando se presentan casos anómalos en la red. Sin embargo, permite a los profesionales de IT analizar y solventar comportamientos anómalos en el tráfico de la red. (Mario, 2013)

2.4.2. Interfaz de Usuario

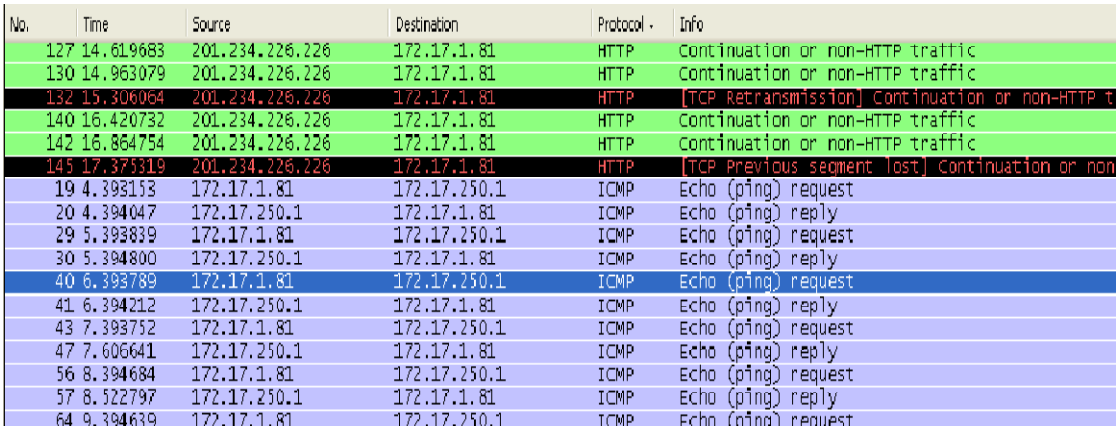
A continuación se muestra y detalla la interfaz de usuario y como se aplican las principales funciones de WireShark (Capturar, Desplegar y Filtrar paquetes).

Existen dos maneras de iniciar la aplicación una es desde la línea de comando (*shell*) y otra desde el entorno gráfico. Cuando se inicia desde la línea de comando se tiene la posibilidad de especificar opciones adicionales que depende de las funciones que se quieran aprovechar.

La interfaz principal de WireShark cuenta con varias secciones:

- El Menú principal es utilizado para iniciar las acciones y/o funciones de la aplicación.

- File, similar a otras aplicaciones GUI este contiene los ítems para manipular archivos y para cerrar la aplicación Wireshark.
- Edit, este menú contiene ítems aplicar funciones a los paquetes, por ejemplo, buscar un paquetes especifico, aplicar una marca al paquete y configurar la interfaz de usuario.
- View, permite configurar el despliegue de la data capturada.
- Go, contiene ítems que permiten el desplazamiento entre los paquetes.
- Capture, para iniciar y detener la captura de paquetes.
- Analyze, contiene ítems que permite manipular los filtros, habilitar o deshabilitar protocolos, flujos de paquetes, etc.
- Statistics, contiene ítems que permiten definir u obtener las estadísticas de la data capturada.
- Help, menú de ayuda.
- Barra de herramientas principal, permite el acceso rápido a las funciones más utilizadas.
- Barra de herramientas para filtros, aquí se especifica el filtro que se desea aplicar a los paquetes que están siendo capturados.
- Panel de paquetes capturados, en este panel se despliega la lista de paquetes capturados. Al hacer clic sobre algunos de estos se despliega cierta información en los otros paneles.



No.	Time	Source	Destination	Protocol	Info
127	14.619683	201.234.226.226	172.17.1.81	HTTP	Continuation or non-HTTP traffic
130	14.963079	201.234.226.226	172.17.1.81	HTTP	Continuation or non-HTTP traffic
132	15.306064	201.234.226.226	172.17.1.81	HTTP	[TCP Retransmission] Continuation or non-HTTP t
140	16.420732	201.234.226.226	172.17.1.81	HTTP	Continuation or non-HTTP traffic
142	16.864754	201.234.226.226	172.17.1.81	HTTP	Continuation or non-HTTP traffic
145	17.375319	201.234.226.226	172.17.1.81	HTTP	[TCP Previous segment lost] Continuation or non
19	4.393153	172.17.1.81	172.17.250.1	ICMP	Echo (ping) request
20	4.394047	172.17.250.1	172.17.1.81	ICMP	Echo (ping) reply
29	5.393839	172.17.1.81	172.17.250.1	ICMP	Echo (ping) request
30	5.394800	172.17.250.1	172.17.1.81	ICMP	Echo (ping) reply
40	6.393789	172.17.1.81	172.17.250.1	ICMP	Echo (ping) request
41	6.394212	172.17.250.1	172.17.1.81	ICMP	Echo (ping) reply
43	7.393752	172.17.1.81	172.17.250.1	ICMP	Echo (ping) request
47	7.606641	172.17.250.1	172.17.1.81	ICMP	Echo (ping) reply
56	8.394684	172.17.1.81	172.17.250.1	ICMP	Echo (ping) request
57	8.522797	172.17.250.1	172.17.1.81	ICMP	Echo (ping) reply
64	9.394639	172.17.1.81	172.17.250.1	ICMP	Echo (ping) request

Figura 2.14 – Panel de paquetes IP capturados

Fuente: Tutorial Wireshark(Mario, 2013)

2.5. Alcances y Limitaciones

Todas las configuraciones y pruebas realizadas bajo el emulador GNS3 con el IOS cisco 2691, cabe mencionar que un enlace virtual es más lento y fácilmente congestionable que uno real. GNS3 trabaja conjuntamente con Dynamips y Dynagen, para realizar el "milagro" de la emulación; estos 3 componentes dotan a un PC tradicional de la capacidad de: conectarse vía Telnet a la consola de un router virtual, realizar capturas de los paquetes que pasan por sus enlaces virtuales, trabajar conjuntamente con varios emuladores para repartir su carga de procesamiento y lo más importante, permite la comunicación con equipos reales externos.

Las capacidades de procesamiento óptimas de emulador GNS3 dependen de la cantidad de routers que se desean emular, es decir, se requerirán más recursos de CPU y memoria RAM si se quieren emular topologías con muchos routers.

Obviamente GNS3 posee algunas deficiencias, como la incapacidad de emular ciertas aplicaciones o la falta de soporte a todas las plataformas CISCO disponible en el mercado, pero al ser una aplicación que está en constante actualización y con gran aceptación en el público, es muy probable que estas carencias se solucionen en un futuro próximo.

CAPÍTULO 3
TECNOLOGÍAS QUE SE PUEDEN SIMULAR CON GNS3

3.1. FrameRelay

FrameRelay es un estándar de la ITU (International TelecommunicationUnion)y el ANSI (American NationalStandardsInstitute) que define el proceso para enviar datos sobre una red pública de datos.

FrameRelay constituye un método de comunicación orientado a paquetes para la conexión de sistemas informáticos. Se utiliza para la interconexión de redes de área local (LAN's) y redes de área extensa (WAN's) sobre redes públicas o privadas. La mayoría de compañías públicas de telecomunicaciones ofrecen los servicios FrameRelay como una forma de establecer conexiones virtuales de área extensa que ofrezcan unas prestaciones relativamente altas.(Teillier)

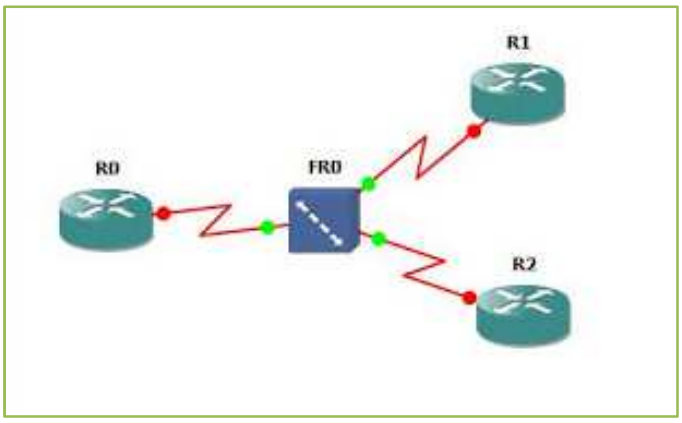


Figura 3.1 -Esquema de una conexión FrameRelay.

Fuente: (Networkeando, 2008)

FrameRelay es una interfaz de usuario dentro de una red de conmutación de paquetes de área extensa, que típicamente ofrece un ancho de banda comprendida en el rango de 56 Kbps y 1.544 Mbps. Las conexiones a una red FrameRelay requieren un encaminador y una línea desde las instalaciones del cliente hasta el puerto de entrada a FrameRelay en la compañía de telecomunicaciones. Esta línea consiste a menudo en una línea digital alquilada como T1 aunque esto depende del tráfico.

A continuación se muestran dos posibles métodos de conexión en área extensa:

Método de red privada.- En este método, cada instalación necesita tres líneas dedicadas (alquiladas) y encaminadores asociados, para conectarse con cualquiera de los otros lugares, con un total de seis líneas dedicadas y 12 encaminadores.

Método de FrameRelay.- En este método de red pública, cada instalación requiere una única línea dedicada (alquilada) y un encaminador asociado dentro de la red FrameRelay.

Los paquetes recibidos de múltiples usuarios se multiplexan sobre la línea y se envían a través de la red FrameRelay a sus destinos.

3.1.1. La Era FrameRelay

FrameRelay se encuentra hoy ya en el corazón de las ofertas europeas de servicios de telecomunicación. Esta nueva tecnología libra una dura y previsiblemente larga batalla con la tradicional X.25 por hacerse con las mayores cuotas del mercado de servicios de conmutación de datos en aplicaciones como interconexión de redes locales, área específica a la que aporta ventajas competitivas indiscutibles. Sin embargo, el viejo mundo X.25 seguirá cosechando los mejores resultados todavía durante muchos años, así lo pronostican diversos estudios y así lo confirman las expectativas de fabricantes y operadores de telecomunicación.Sin embargo, su idoneidad para determinadas soluciones corporativas, como interconexión de LAN's y transporte de tráficos SNA, está representando un importante muro de contención a la tan anunciaday ahora parece que postergada eclosión ATM. (Teillier)

3.1.2. Servicios

Entre los servicios FrameRelay ofrecidos por operadores de telecomunicaciones existen muchos elementos comunes. Una de las tendencias que rigen este mercado es la provisión actual o futura de servicios de extremo a extremo; es decir, el transporte de los datos de un usuario a otro queda asegurado, administrando además si llega el caso de los routers de acceso situados en las instalaciones de los clientes.

3.1.3. InteroperatividadFrameRelay / ATM

FrameRelay/ATM Network Internetworking permite a los usuarios finales de dispositivos o redes FrameRelay comunicar entre sí a través de una red ATM sin necesidad de efectuar ningún cambio de equipamiento. La interoperatividad de red se produce cuando se utiliza un protocolo en cada extremo de la transmisión y otro distinto en el camino entre ambos puntos. En un punto de la red, y de forma totalmente transparente para el usuario, los paquetes FrameRelay son segmentados en celdas ATM, que a su vez, serán reagrupadas en paquetes FrameRelay antes de alcanzar su destino.

Como es lógico, para que ello sea posible es preciso compensar las diferencias entre ambas tecnologías, operación que corre a cargo de InterworkingFunction (IWF), localizada generalmente en los conmutadores situados en las fronteras de los servicios FrameRelay y ATM.

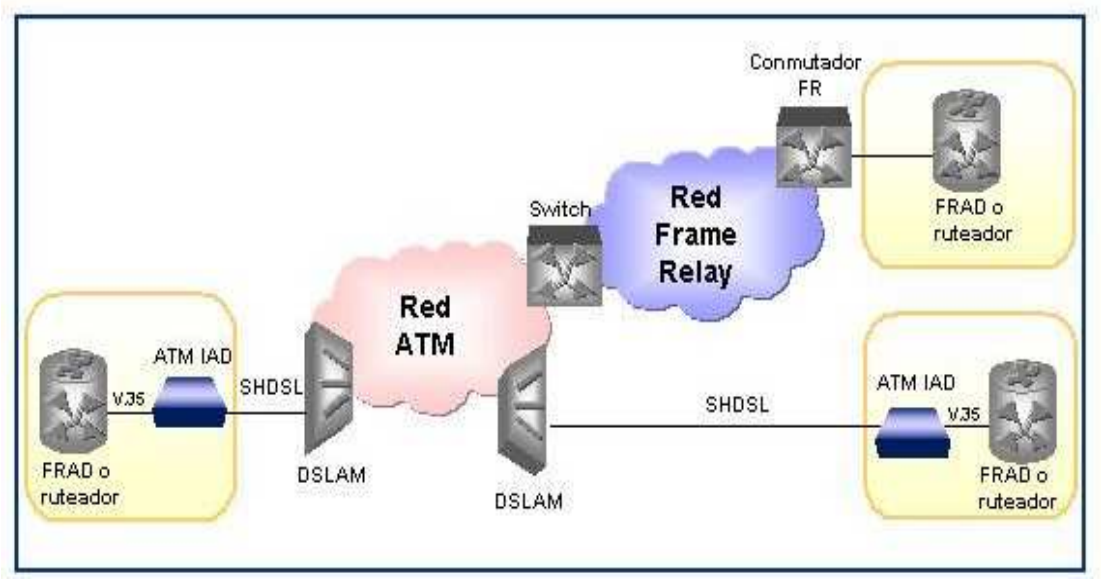


Figura 3.2 - Modelo de FrameRelay sobre ATM.

Fuente: http://www.oocities.org/es/marbry69/e3/T_2.htm

Los dispositivos de acceso integrados (IAD) ATM Link Access (LA) permiten efectuar la convergencia de servicios múltiples, tales como voz, LAN y datos sobre una línea de acceso DSL, utilizando la red ATM y DSLAM existentes. Los IAD basados en ATM garantizan la calidad del servicio (QoS) y la gestión de punta a punta hasta el establecimiento del cliente.

En este modelo se utiliza la interfaz V.35 y el soporte de interconexión de FrameRelay (FRF.5) e interconexión de servicios (FRF.8), ya que cuando un equipo conectado mediante una FrameRelay quiere transmitir a un equipo conectado a una ATM mediante ATM, se tienen que desempaquetar los datos, cambiar el formato y empaquetar otra vez según su tipo de conexión.(Martínez, 2009)

3.2. MPLS (MultiprotocolLabelSwitching)

MPLS es un mecanismo de transporte de datos estándar creado por la IETF (Internet EngineeringTaskForce) y definido en el RFC 3031.

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. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

MPLS es una tecnología híbrida que intenta combinar las mejores características de las técnicas conocidas para hacer llegar un paquete de un origen a un destino, tanto de capa 2 (Switching) como de capa 3 (Routing), a través de una red de interconexión.(GALLEGOS, 2012)

3.2.1. Antecedentes de MPLS

La demanda de los usuarios de nuevos servicios y la necesidad del aumento de ancho de banda impulsó en un inicio a los proveedores de servicios de Telecomunicaciones a desplegar en sus infraestructuras una combinación de enrutadores IP con conmutadores ATM/FrameRelay, una vez consolidada la tecnología TCP/IP, esta combinación propiciaba un equilibrio frente a las necesidades de crecimiento de la época.

Este modelo de red adoptado presentó limitaciones de interoperabilidad con otras redes, dificultad de gestionar estas conexiones y un alto crecimiento en equipamiento. Para suplir estas necesidades a mediados de la década de los 90 empezaron a aparecer soluciones de conmutación de nivel 2 diseñadas con la idea de tomar el software de control de un router con el objeto de integrar el rendimiento de reenvío con el cambio de etiqueta de un switch ATM para crear un router extremadamente rápido y eficiente.

Tras establecerse el grupo de trabajo MPLS del IETF en 1998 se definió un estándar para unificar las soluciones que presentaron algunos fabricantes conocido también como MPLS y

recogido en la RFC 3031. Actualmente es una tecnología que para el operador representa la factibilidad de poder ofrecer a sus usuarios servicios multimedia desde una plataforma de red común y basada en cualquier tecnología de transporte a nivel físico y de enlace como por ejemplo: ATM, FrameRelay, SDH/SONET o la tendencia actual DWDM y otras, garantizando transparencia y Calidad de Servicio gracias al manejo de dos planos uno para enrutamiento y otro para la conmutación de etiquetas a nivel local dentro de la red.(PUPIALES, 2012)

3.2.2. Definición General de MPLS

MPLS es una tecnología que combina las funciones de enrutamiento de capa 3 con las funciones de envío de capa 2, por esta razón se lo denomina Multiprotocolo ya que brinda la posibilidad de trabajar con cualquier tecnología de transporte ya sea a nivel de enlace o físico y con aplicaciones que están sobre el nivel de red. La Conmutación de etiquetas (LabelSwitching) permite identificar una clasificación de tráfico, encaminando a esta clasificación por un determinado camino virtual brindando QoS y otras ventajas que serán descritas a lo largo del presente capítulo.

3.2.2.1. Ventajas de MPLS frente a tecnologías anteriores

MPLS surgió como un estándar emergente para agrupar distintas soluciones de conmutación multinivel presentadas por los diferentes fabricantes.

Un modelo que se impuso con anterioridad fue el IP/ATM, que al inicio satisfacía los requisitos de las nuevas aplicaciones ya que utilizaba el encaminamiento inteligente de nivel 3 de los routers IP basándose en la alta velocidad de los conmutadores de nivel 2 y los circuitos permanentes virtuales de los switches ATM en la red troncal. Sin embargo esta integración presentó ciertas limitaciones debido a la dificultad de operar e integrar una red basada en dos tecnologías diferentes concebidas para finalidades distintas como son:

- Problemas en la separación de las funciones de ruteo con las funciones de conmutación.
- Complejidad en la gestión de dos redes separadas y tecnológicamente diferentes, una infraestructura de topología real de conmutadores ATM sobre una red lógica IP lo que conduce a mayores costos en la gestión de las redes.

- Por el tamaño pequeño de la celda (53 bytes) para la transmisión representa un overhead del 20%, ya que por cada celda enviada se tiene que analizar la cabecera (identificación de canal, detección de errores, etc.) lo que podría ser utilizado por la carga útil, en consecuencia se reduce en este mismo porcentaje el ancho de banda disponible.
- Problemas de interoperabilidad de los productos de diferentes fabricantes.

Esta última se dio debido a que los fabricantes decidieron buscar soluciones a estos inconvenientes por su propia cuenta para el mejoramiento de este modelo de red.

Las técnicas que se desarrollaron previas a la estandarización de MPLS fueron:

- IP Switching de Ipsilon Networks
- Tag Switching de Cisco.
- Aggregate Route-Base IP Switching (ARIS) de IBM.
- IP Navigator de Cascade/Ascend/Lucent.
- Cell Switching Router (CSR) de Toshiba.

Estas soluciones contribuyeron de manera significativa al desarrollo de MPLS como un estándar del IETF y por tanto son consideradas como un valioso aporte a esta tecnología.(PUPIALES, 2012)

3.2.2.2. Características

A continuación se describen las características más importantes de la tecnología MPLS:

- Fue diseñada para operar cualquier tecnología de transporte a nivel de enlace, no solamente ATM facilitando la migración a las redes de próxima generación.
- MPLS es una tecnología que combina eficazmente las funciones de control de ruteo con la simplicidad y rapidez de la conmutación de nivel 2.
- La implementación de MPLS permite a una red ser más sencilla de operar, mayor escalabilidad e interoperabilidad debido al soporte de diversas tecnologías bajo una plataforma común.
- Utiliza protocolos para intercambio y distribución de etiquetas que permite la creación de caminos virtuales conocidos como LSP (LabelSwitchedPath).
- MPLS permite aplicar técnicas de Ingeniería de Tráfico para encontrar la mejor ruta no necesariamente la más corta en algunos casos, pero que garantiza la llegada de los flujos de tráficos evitando cuellos de botella y caída de los enlaces.

3.2.3. Elementos Básicos de Mpls

Los elementos más comunes y fundamentales para la comprensión de MPLS son los siguientes:

- LER, LabelEdgeRouter (Ruteador Etiquetador de Borde)
- LSR, LabelSwitchingRouter (Ruteador de Conmutación de Etiquetas)
- LSP, LabelSwitchedPath (Ruta Conmutada de Etiquetas)
- FEC, Forward EquivalenceClass (Clase Equivalente de Envío)
- LIB, LabelInformation Base (Base de Información de Etiquetas)
- LDP, LabelDistributionProtocol (Protocolo de Distribución de Etiquetas)

En la figura 3.3 se presenta una red básica con MPLS en la que se indican los ruteadores de borde LER, y el ruteador de conmutación de etiquetas LSR dentro de un dominio MPLS. (PUPIALES, 2012)

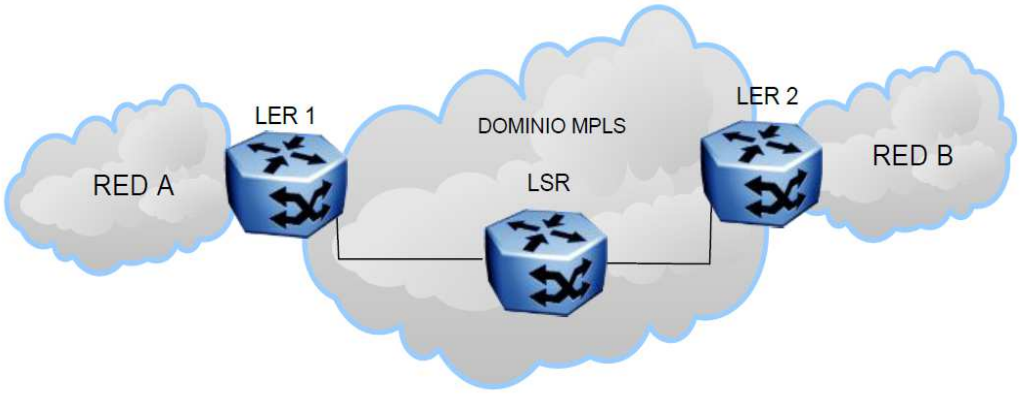


Figura 3.3- Red básica MPLS

Fuente: http://repositorio.utn.edu.ec/handle/123456789/4

3.2.3.1. LabelEdgeRouter (LER)

Los LER se encuentran ubicados en el borde de la red MPLS y desempeñan las funciones de encaminamiento tanto para un dominio MPLS como para un dominio no MPLS (otras redes). El propósito de los LER es el análisis y clasificación del paquete IP que entra a la red de acuerdo a criterios (que se explican posteriormente), a esta clasificación por conjuntos de paquetes se le denomina FEC58. Una vez analizado el paquete IP se añade una cabecera MPLS y en uno de sus campos denominado Etiqueta se le asigna un valor de acuerdo a su clasificación FEC.

Al salir del dominio MPLS el LER de salida es el que direcciona el paquete a la red de destino por enrutamiento convencional eliminando la cabecera MPLS. El LER de ingreso a la red o dominio MPLS también se lo conoce como Ingress LSR y el LER de salida se lo llama Egress LSR.

3.2.3.2. LabelSwitchingRouter (LSR)

El LSR se encuentra ubicado en el núcleo de la red MPLS, realiza encaminamiento basándose en la conmutación de etiquetas. Una vez que le llega un paquete a una de sus interfaces éste lee la etiqueta de entrada en la cabecera MPLS y busca en la tabla de conmutación la etiqueta y la interfaz de salida para designar la nueva etiqueta que indica el siguiente salto dentro del dominio y finalmente reenvía el paquete por el camino ya designado en el LER (según el FEC).

3.2.3.3. Forward EquivalenceClass (FEC)

El FEC es un conjunto de paquetes que son reenviados sobre un mismo camino a través de la red (LSP) y se determina una vez a la entrada a la red MPLS en un router LER. Para clasificar a los paquetes dentro de un mismo FEC se lo hace en base a criterios como:

- Dirección IP de origen, destino o direcciones IP de la red.
- Número de puerto de origen o destino
- Campo protocolo de IP (TCP, UDP, ICMP60, etc.)
- Valor del campo DSCP de DiffServ
- Etiqueta de flujo en IPv6

Cada FEC tiene QoS debido a que se debe tratar a los paquetes que van por el mismo camino de diferente manera, dando prioridad según la necesidad de manera que se utilizan los recursos de la red óptimamente.

Agregación

La Agregación es un mecanismo que permite agrupar varios FEC mediante la asignación de una sola etiqueta para todos, de esta manera se reduce el tiempo de envío de los FEC porque se elimina asociaciones etiqueta/FEC redundantes.

Puede ser posible la Agregación cuando a un LSR le llegan desde un mismo LER varios FEC con el mismo origen y destino dentro de la red MPLS asignados al mismo camino LSP.

En la figura 3.4 se puede observar que para tres FEC hay tres asociaciones etiqueta/FEC sin la utilización de la Agregación, pero al utilizarla, el FEC se convierte en un conjunto de otros FEC con características comunes teniendo así una sola asociación etiqueta/FEC.

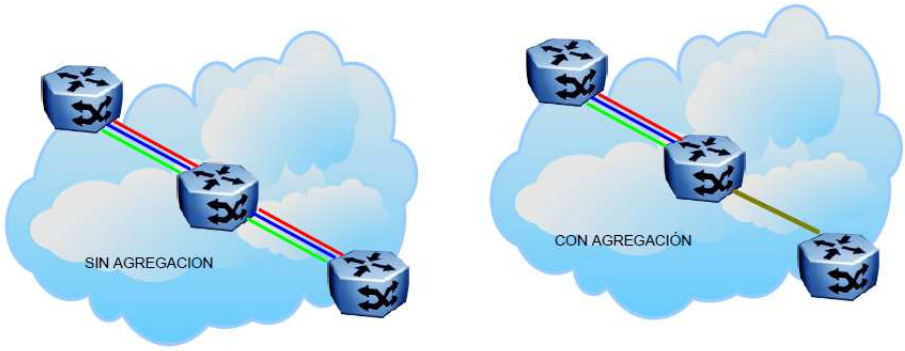


Figura 3.4- FEC sin Agregación y con Agregación
Fuente: http://repositorio.utn.edu.ec/handle/123456789/4

3.2.3.4. LabelDistributionProtocol (LDP)

El LDP define los mecanismos para la distribución de etiquetas, permite a los LSR descubrirse e intercambiar información sobre las asociaciones FEC/Etiqueta que se han realizado y sobre todo para mantener la coherencia de las etiquetas utilizadas para los distintos tipos de tráfico que conmutan. Con este protocolo se evita que a un LSR le llegue tráfico con una etiqueta que no se encuentra en su tabla, con esto se asegura la rapidez en la conmutación de los LSR.

Para establecer la ruta LSP (LabelSwitchedPath) los LER/LSR establecen sesiones a través de mensajes en los cuales se solicita:

- A su vecino que le informe sobre que etiqueta debe usar para el envío del tráfico por una determinada interfaz, es decir que la distribución de etiquetas se realiza contraria al camino que sigue el tráfico.
- Un LER/LSR informa de las asociaciones Etiqueta/FEC a sus vecinos que las almacenan en sus tablas sin haber solicitado la información, este mecanismo es más eficaz ya que así todos los vecinos LER/LSR mantienen las tablas actualizadas (del

mismo LSP) y haciendo el proceso de conmutación de etiquetas mucho más rápido pero incrementando el tráfico de control.

MPLS asume algunos Protocolos de Distribución de Etiquetas estandarizados como: RSVP del Modelo de Servicios Integrados de IETF, TDP (TagDistributionProtocol) de Cisco o CR-LDP (ConstrainedRouting LDP), siendo el primero el más común.

3.2.3.5. LabelSwitchedPath (LSP)

El LSP es una ruta de tráfico específica a través de la red MPLS que sigue un grupo de paquetes que pertenecen al mismo FEC. Esta ruta se crea concatenando los saltos que dan los paquetes para el intercambio de etiquetas en los LSR y para esto utiliza mensajes LDP. Los mensajes utilizados por los LSR son los siguientes:

- Descubrimiento: mediante mensajes *"hello"* de un LSR a otro LSR.
- Sesión: dos LSR establecen y mantienen la comunicación.
- Anuncio: para dar a conocer a otro LSR de las asociaciones FEC/Etiqueta.
- Notificación: información de eventos y errores

Las rutas LSP se forman desde el destino hacia el origen debido a que el LSR de origen genera las peticiones para crear un nuevo LSP mientras que el destino responde a estas solicitudes formándose de esta manera el LSP hasta el origen. Existen dos métodos para el establecimiento de los LSP's:

1. Ruta explícita:

A partir del primer LSR de salto se construye una lista de saltos específica utilizando los protocolos de señalización o de distribución de etiquetas (RSVP, LDP, etc.).

2. Salto a Salto:

Cada LSR selecciona el próximo salto según el FEC que esté disponible.

El encaminamiento del LSP se realiza mediante protocolos de enrutamiento que utilizan algoritmos de estado de enlace para conocer la ruta trazada completa y tener rutas alternativas si algún enlace falla.

3.2.3.6. LabelInformationBase (LIB)

Un LSR o LER tiene dos tablas, una dedicada a la información de enrutamiento y la segunda con la información a nivel local de las etiquetas conocida como LIB. Los datos de la taba LIB se relacionan con las etiquetas que han sido asignadas por un LER/LSR y de las

asociaciones etiqueta/FEC recibidas de los vecinos del dominio MPLS mediante los protocolos de Distribución de Etiquetas.

La construcción de estas tablas se basa en las operaciones que realizan las etiquetas y son las siguientes:

- PUSH: imposición de las etiquetas en un ruteador de ingreso LER.
- SWAP: la etiqueta es cambiada por otra dentro del mismo rango que identifica un FEC en los LSR's.
- POP: operación en la que se elimina la etiqueta en un LER al salir de la red MPLS.

La información que proporciona una tabla LIB da a conocer sobre la interfaz y etiqueta de entrada seguida de la interfaz y el valor de etiqueta de salida, este proceso se realiza en cada salto de un LSR o LER y permite mantener actualizadas las rutas LSP. En la tabla 3.1 se muestra un ejemplo de la información que tiene una tabla LIB.

Tabla 3.1 Ejemplo de la información proporcionada por una tabla LIB

Interfaz de Entrada	Etiqueta de Entrada	Interfaz de Salida	Etiqueta de Salida
1	60	3	75
2	90	1	80

Fuente: http://repositorio.utn.edu.ec/handle/123456789/4

3.2.4. Encabezado de Mpls

En la figura 3.5 se presentan los campos de la cabecera genérica MPLS que se asigna una vez a la entrada en el router LER.

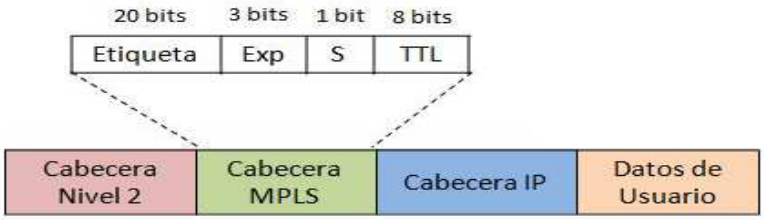


Figura 3.5- Estructura genérica de la cabecera MPLS

Fuente: http://repositorio.utn.edu.ec/handle/123456789/4

Como se observa en la figura 2.5 la cabecera MPLS está formada de 32 bits distribuidos en cuatro campos que son:

- **Etiqueta:** identifica a que conjunto de FEC está asignado el paquete y mediante este los ruteadores deciden por donde encaminar el paquete o que LSP debe seguir.
- **Exp (Experimental):** bits de uso experimental cuya proyección es la utilización para QoS aplicando Calidad de Servicio para asignar un nivel de prioridad a cada paquete.
- **S (Stack):** para apilar las etiquetas en forma jerárquica, si S vale 1 se trata de la última etiqueta en la pila (primera en ingresar a un dominio MPLS), caso contrario S vale 0. En caso de existir una sola etiqueta el valor de S es 1.
- **TTL (Time To Live):** cumple con una función similar a la del campo TTL de IPv4. Cuando a un paquete se le asigna la cabecera MPLS el campo TTL copia el valor TTLdel paquete IP pero reducido en una unidad en el LER y por cada salto que realice en el dominio MPLS. Este mecanismo permite reducir la posibilidad de bucles en la red. (PUPIALES, 2012)

3.2.5. Descripción Funcional de Mpls

La conmutación multinivel que realiza MPLS se basa fundamentalmente en la separación de dos funciones que a su vez están efectivamente coordinadas, estas funciones se las conoce como:

- Plano de Control
- Plano de Envío

Los routers o switches que soportan MPLS trabajan en estos dos planos, específicamente los LER al ser el borde del dominio MPLS cumplen con estas dos funciones de encaminamiento y de envío inicial de los paquetes asignando una cabecera MPLS mientras que los LSR solo se encargan de la conmutación de las etiquetas.(Ghein, 2007)

3.2.5.1. Funcionamiento del Plano de Control

El Plano de Control utiliza los protocolos de enrutamiento ya sean de vector distancia o estado de enlace, para el intercambio de información dentro de la red MPLS, permitiendo la construcción y mantenimiento de las tablas de enrutamiento que proporcionan las características de la topología, patrón de tráfico o detalles de

losenlaces. De esta manera se mantiene coherencia entre los LER y LSR evitando que a un determinado LSR le llegue un paquete con una etiqueta para el cual no tiene entrada en su tabla.

La difusión de las tablas de enrutamiento a los vecinos es muy importante porque establece los caminos virtuales LSP que los LER indican al inicio para la generación de las tablas de envío utilizando también la señalización que proveen los Protocolos de Distribución de Etiquetas (RSVP, LDP o TDP) y posteriormente el intercambio de etiquetas (Plano de Envío). Al tener la tabla de encaminamiento actualizada se escoge la dirección del próximo salto permitiendo el cálculo de las mejores rutas dentro de la red MPLS y caminos emergentes en caso de fallos.

3.2.5.2. Funcionamiento del Plano de Envío

El Plano de Envío MPLS utiliza la información de las etiquetas para la conmutación local de las mismas y para el envío de los paquetes a sus vecinos dentro del dominio, es decir se encarga de las asignaciones y modificaciones de etiquetas rigiéndose a la información proporcionada por el Plano de Control.

El paquete conforme avanza dentro de la red MPLS adquiere una nueva etiqueta, el valor de esta etiqueta define el FEC (Forward EquivalenceClass) asignado. En la figura 3.6 se puede apreciar el intercambio de etiquetas de un paquete.

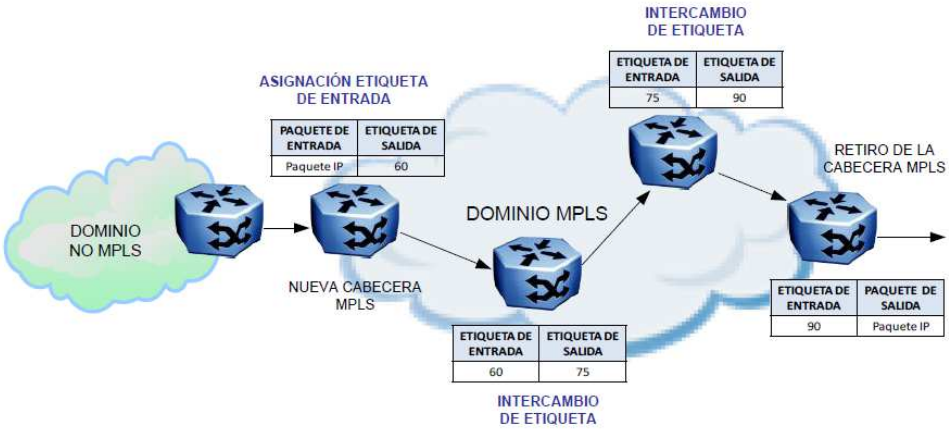


Figura 3.6 -Intercambio de Etiquetas de un dominio MPLS

Fuente: http://repositorio.utn.edu.ec/handle/123456789/4

Como se observa en la figura 3.6 un paquete de cualquier otra red (dominio no MPLS) ingresa a la red MPLS, el router de borde LER es el encargado de analizar el paquete y clasificarlo a un determinado FEC, luego al añadirle una cabecera MPLS el campo etiqueta tiene un valor de acuerdo a su FEC consultando con la tabla de enrutamiento envío para este caso la etiqueta de salida es 60.

Posteriormente tras la asignación de la cabecera MPLS el paquete realiza su siguiente salto a otro LSR y éste consulta en su tabla de envío y observa que la etiqueta de entrada es 60 y le asigna una nueva con el valor de 75, el siguiente LSR realiza la misma acción y tiene como etiqueta de entrada 75 y de salida 90. Al llegar el LER de salida para éste la etiqueta de entrada es 90 pero su función es la de retirar la cabecera MPLS y enviar al paquete utilizando enrutamiento convencional (tabla de enrutamiento).

En resumen los LSR´s solo analizan el campo "etiqueta" para buscar y localizar si en su tabla se encuentra la etiqueta de entrada, una vez localizada esta etiqueta es modificada por una nueva a su salida por una determinada interfaz. El camino que siguen los paquetes (LSP) se forma a través de cada salto en un solo sentido, para un tráfico dúplex se requiere la creación de dos LSP's, uno en cada sentido.

3.2.6. Aplicaciones de MPLS

MPLS es una tecnología abierta y esta a su vez proporciona muchas aplicaciones a nivel de redes troncales.

Entre las aplicaciones más comunes de MPLS tenemos:

- Ingeniería de Trafico.
- Calidad de Servicio.

3.2.6.1. Ingeniería de Tráfico

Es una facilidad que ofrece MPLS para adaptar los flujos de tráfico a los recursos físicos de la red, equilibrando de forma óptima la utilización de los mismos, de manera que no haya recursos utilizados excesivamente, con lo que se provocaría cuellos de botella y colapso de los enlaces.

Con la Ingeniería de Tráfico es factible desviar parte del tráfico cursante por otro camino alternativo menos congestionado aunque no sea la ruta más corta, teniendo el administrador de la red la posibilidad de:

1. Establecer rutas explícitas especificando el camino LSP exacto (cobre, fibra óptica, etc.)
2. Rutas restringidas para el caso de servicios especiales.
3. Calcular la ruta más eficiente en base a los requerimientos y restricciones.
4. Obtener informes estadísticos sobre el tráfico que cursa constituyendo una herramienta eficaz para el análisis de la distribución de los recursos de la red y para una planificación futura.

3.2.6.2. Calidad de Servicio

La calidad de servicio se define por la UIT como el efecto global de la calidad del funcionamiento de un servicio que determina el grado de satisfacción de un usuario de dicho servicio.

Nos permite controlar alguna de las características que influyen en la transmisión de un paquete como el ancho de banda, latencia, jitter, las pérdidas de los paquetes en la red, retardos, etc. garantizando la disponibilidad del servicio.

En MPLS la calidad de servicio está dada por la priorización que se da a los flujos de tráfico conocidos como FEC y también por la posibilidad de aplicar técnicas de Ingeniería de Tráficopara descongestionar la red despachando el tráfico por rutas seguras (LSP) y sin mayores demoras.

3.3. VPN (VirtualPrivateNetwork)

Una Red Privada Virtual es una red de información privada que utiliza una infraestructura de Telecomunicaciones pública y conecta a usuarios de forma remota hacia una red principal, siendo una solución ideal para las empresas, y su objetivo es brindar aplicaciones Intranet y Extranet integrando soluciones multimedia.

Las VPN’s tradicionales ya sean basadas en PVC(Circuitos Virtuales Permanentes) o túneles IP han sido de gran beneficio pero tienen ciertos inconvenientes que pueden ser resueltos con la utilización de MPLS.

Las VPN’s basadas en PVC utilizan la infraestructura de las redes ATM o FrameRelay y los PVC’s se establecen entre los nodos de extremo a extremo con la configuración manual de cada uno, lo que implica complejidad en la gestión de la red del proveedor ya

que se trata de una topología lógica mallada sobrepuesta a la red física y al agregar un nuevo miembro a la VPN es necesario restablecer todos los PVC's.(PUPIALES, 2012)

3.3.1. Ventajas y desventajas de las VPN's

Las IP VPN están basadas en Protocolos de Túnel como por ejemplo IPSec68, la información se cifra y se encapsula en una nueva cabecera IP. La desventaja en este tipo de implementaciones se da porque se ocultan las cabeceras de los paquetes originales y las opciones de QoS son bastante limitadas ya que no se puede distinguir los flujos por aplicación dificultando la asignación de los diferentes niveles de servicio.

En general los inconvenientes más comunes que tienen las VPN tradicionales son las siguientes:

- Se basan en conexiones punto a punto (PVC o túneles).
- La configuración de cada nodo de la VPN es manual y cada vez que se integra uno supone la reconfiguración de todos los anteriores.
- La Calidad de Servicio se ofrece hasta cierta parte, más no durante el transporte.
- El modelo topológico sobrepuesto a la red existente implica poca flexibilidad en la provisión y gestión del servicio.

Utilizando MPLS para implementar VPN's se eliminan los inconvenientes de las tecnologías anteriores. En primera instancia el modelo topológico que se crea no se sobrepone sino se acopla a la red del proveedor, esto elimina las conexiones extremo a extremo (túneles IP convencionales o circuitos virtuales) y los túneles se van creando con el intercambio de las etiquetas formándose así los LSP que vendrían a ser los "túneles MPLS".

Las ventajas que se tiene con MPLS son:

- Se elimina la complejidad de los túneles y los PVC's.
- Para la implementación no es necesario realizar cambios en todos los puntos involucrados como ocurre con las VPN's tradicionales por lo contrario solo se configura a nivel del proveedor evitando tareas complejas y riesgosas.
- Las garantías de Calidad de Servicio se mantienen de extremo a extremo separando los flujos de tráfico por clases.

- Para aumentar la seguridad se pueden utilizar los protocolos de encriptación manejados también por las VPN's tradicionales como IPSec (Internet Protocol Security).
- Con la Ingeniería de Tráfico que ofrece MPLS se garantiza que en el servicio VPN no influyan parámetros que afecten la calidad de extremo a extremo.

3.3.2. Generalidades de la Arquitectura de las VPN/MPLS.

Una VPN/MPLS básica está formada de tres elementos físicos que son: P (Provider) o router interno del proveedor, PE (ProviderEdge) o router frontera del proveedor y CE (CustomerEdge) denominado así al router frontera del cliente. Además existen dos aspectos internos de la arquitectura de las VPN soportadas en MPLS que son: el RouteDistinguisher y el Route Target, mecanismos que permiten distinguir los requerimientos del cliente suscrito a una VPN.

3.3.2.1. RouteDistinguisher

Los routers PE (ProviderEdge) se conectan a los routers CE (CustomerEdge) y distribuyen la información que contienen sobre las VPN's a otros routers PE a través del protocolo MP-BGP o Multiprotocolo BGP, en este intercambio de información el router PE agrega como prefijo a la dirección IPv4 una cantidad de 64 bits conocidos como RouteDistinguisher lo que permite a la dirección IPv4 hacerla globalmente única (ruta privada) y resultando finalmente una dirección de 96 bits denominada VPNv4.

3.3.2.2. Route Target

El Route Target o ruta objetivo es un atributo adicional colocado a las rutas VPNv4 vía BGP que permite identificar la membrecía de un cliente a una VPN cuando algunos sitios de cliente participan en más de una VPN. El Route Target se introdujo en la arquitectura de las VPN/MPLS para soportar topologías más complejas.
Cada enrutador PE define un valor numérico llamado Route Target que pueden ser:

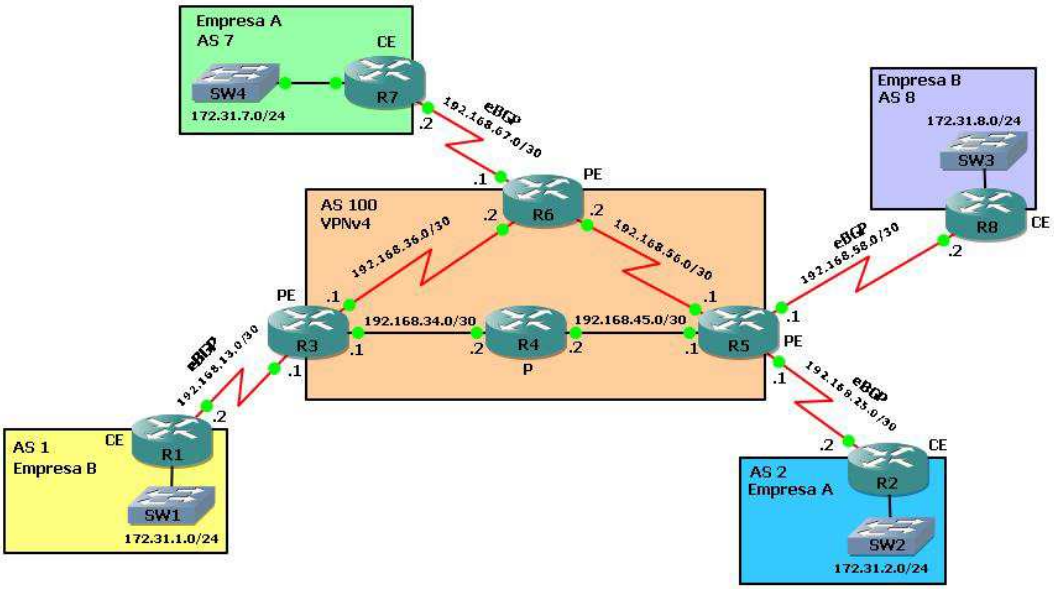


Figura 3.7 - Arquitectura general de una Red VPN/MPLS

Fuente: http://netandsec.xtrweb.com/?tag=networking

Como se observa en la figura 3.7 se ha implementado una topología montada bajo routers Cisco, más GNS3 debido a la cantidad de dispositivos que hay que se desean integrar. Esta topología está basada en una red MPLS VPN, que suele ser la más utilizada.

3.4. VPLS (Virtual Private LAN Service)

3.4.1. Descripción

Un servicio basado en tecnología VPLS es un servicio que emula la funcionalidad completa de una Red de Área Local tradicional independientemente de su distribución geográfica. Dicho de otro modo, una red VPLS convierte los entornos tradicionalmente considerados WAN en entornos LAN.

Un entorno WAN se considera habitualmente con elementos de un cliente o servicio que se conectan a la red individualmente y por norma general situados a gran distancia del primer nodo de red. Así, se crea un enlace punto a punto entre dicho elemento y el primer punto de la red, proporcionando la conectividad al equipo remoto con la Red Privada Virtual.

Con los protocolos tradicionales sobre los que se constituyen Redes Privadas Virtuales suele ser necesario configurar conexiones entre todos y cada uno de los equipos remotos

conectados individualmente, o haciéndose valer de un equipo central que haga de repetidor del tráfico entre el resto de sedes o equipos remotos.

Aun así, es bastante costoso a nivel de recursos lógicos de la red proporcionar conectividad todos con todos, con conexiones punto a punto entre todos los elementos de cada uno de los usuarios o clientes.

A través de una red basada en tecnología VPLS convertimos el entorno WAN, en un entorno LAN, entendiendo este entorno LAN conseguido con VPLS como la simulación de un segmento Ethernet en el que se considera que todos los elementos están directamente conectados entre sí.

Una red VPLS reproduce el funcionamiento de un switch tradicional, elemento de red con el que se separan dominios de colisión, y a través del cual se consigue ampliar un simple segmento Ethernet de red.

VPLS en sí mismo está basado en los protocolos que forman la tecnología MPLS. De este modo, la red se construye sobre la pila de protocolos definida para MPLS, consiguiendo una red IP/MPLSque proporcionará conectividad a los clientes de forma independiente y conectando sus segmentos de red de forma transparente como si estuvieran ubicados en el mismo emplazamiento físico.

Las Redes de Área Local de los clientes se extienden hasta el proveedor de servicios, y se conectan a la red que está simulando el comportamiento de un switch tradicional.

VPLS es un servicio que proporciona la posibilidad de crear Redes Privadas Virtuales sobre estructuras basadas en Ethernet. Consigue que varios segmentos de LAN dispersos geográficamente se comuniquen entre sí compartiendo el mismo dominio de difusión Ethernet, es decir, como si estuvieran conectados al mismo segmento de LAN.

Con la implementación de una red basada en VPLS, las Redes de Área Local de los usuarios se interconectan entre sí como si la red completa fuera un simple switch. Al estar simulando una LAN, se consigue el modelo de conectividad punto a multipunto, en el que todos los segmentos de LAN se comportan como uno único.(Orihuela)

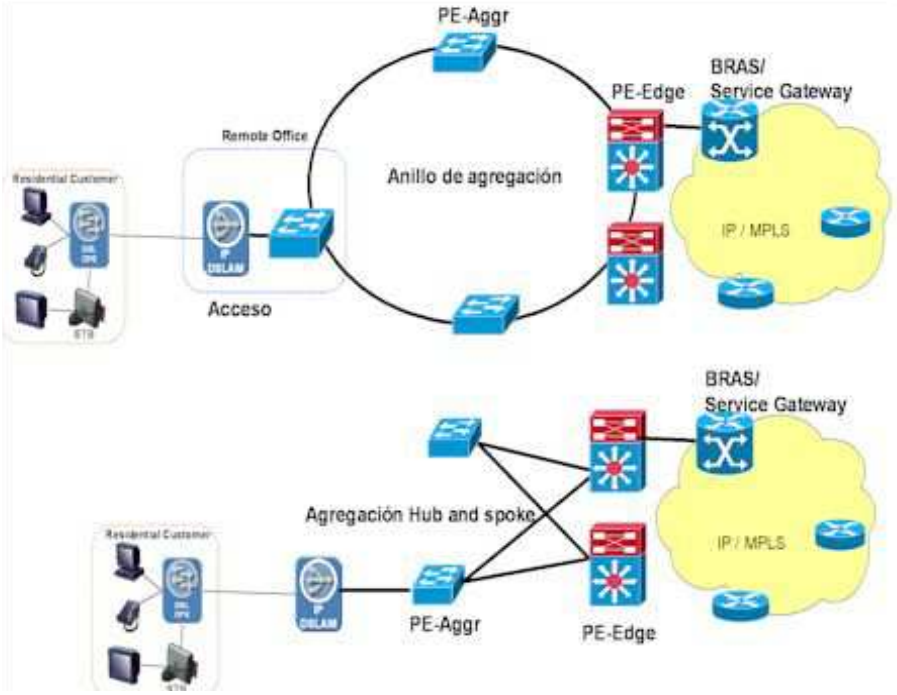


Figura 3.8 – Esquema de una conexión VPLS

Fuente: http://www.oas.org/en/citel/infocitel/2007/enero/multiservicio_e.asp

3.4.2. Elementos de Red

Los elementos de una red VPLS o MPLS se diferencian fundamentalmente por el tipo de conexiones que tienen y su localización lógica en la topología de la red. La distinción se hace radicalmente en si el equipo tiene conexiones contra equipos de usuarios finales, o si solamente tiene conexiones contra equipos dentro de la red.

A los primeros se les denomina **PE router**(ProviderEdgerouter), y son los nodos que ofrecen interfaces de cara al usuario remoto para que éstos puedan acceder a la red. En cierto modo son la frontera de la red MPLS, normalmente la frontera entre un operador de red y sus clientes. Estos equipos desempeñan un papel clave ya que, aun teniendo muy diferenciadas las funciones de red y las funciones de acceso, deben relacionarlas correctamente y crear el servicio de red privada virtual para el usuario basándose en la tecnología aplicada sobre ellos.

Los equipos en el interior de la red, con sólo conexiones troncales entre otros nodos de red, son denominados **P router**(Provider), y mantienen la señalización para el tráfico de

todos los usuarios, utilizando la pila de protocolos correspondiente para diferenciarlo y aislarlo adecuadamente.

Finalmente, para completar la nomenclatura de los equipos involucrados en redes que soportan VPN's sobre IP/MPLS, denominamos a los equipos de los usuarios o clientes como **CE router**(CustomerEdge). Éstos pueden implementar distintas arquitecturas, switches, routers, hosts con capacidad para enrutamiento…en el presente diseño se especificarán recomendaciones para utilizar fundamentalmente routers, y en su caso switches.(Ghein, 2007)

3.5. VLAN'S (Virtual LAN)

3.5.1. Concepto de VLAN

Una VLAN (acrónimo de Virtual LAN "Red de Área Local Virtual") es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLAN's pueden coexistir en un único switch físico, son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local.(Edson Alexander Hernández Gámez, 2012)

3.5.2. Ventajas de las VLAN

Hay muchas ventajas a usar VLAN en una organización, algunas de las cuales se incluyen los siguientes:

Aumento del rendimiento: Al reducir el tamaño del dominio de Broadcast, los dispositivos de red funcionan más eficientemente.

Mayor capacidad de gestión: La división de la red en grupos lógicos de usuarios, aplicaciones o servidores le permite comprender y gestionar mejor la red.

Mayor seguridad: El límite de VLAN marca el final de una subred lógica, para llegar a otras subredes (VLAN), debe pasar a través de un router.

VLAN de voz

Switches de Cisco ofrece una característica única llamada VLAN de voz,alternativamente llamado VLAN auxiliar. La función de la VLAN de voz es permitir la superposición de una topología de voz sobre una red de datos sin problemas, las VLAN de voz proporcionan diferentes redes lógicas, a pesar que los datos y la infraestructura de voz son físicamente iguales.

Nota. La VLAN de voz permite la separación lógica de tráfico de voz desde teléfonos IP y dispositivos de red de voz, sobre la misma red datos física, la VLAN de voz es opcional.

En la figura 3.9 se muestra en ejemple de creación de VLAN.

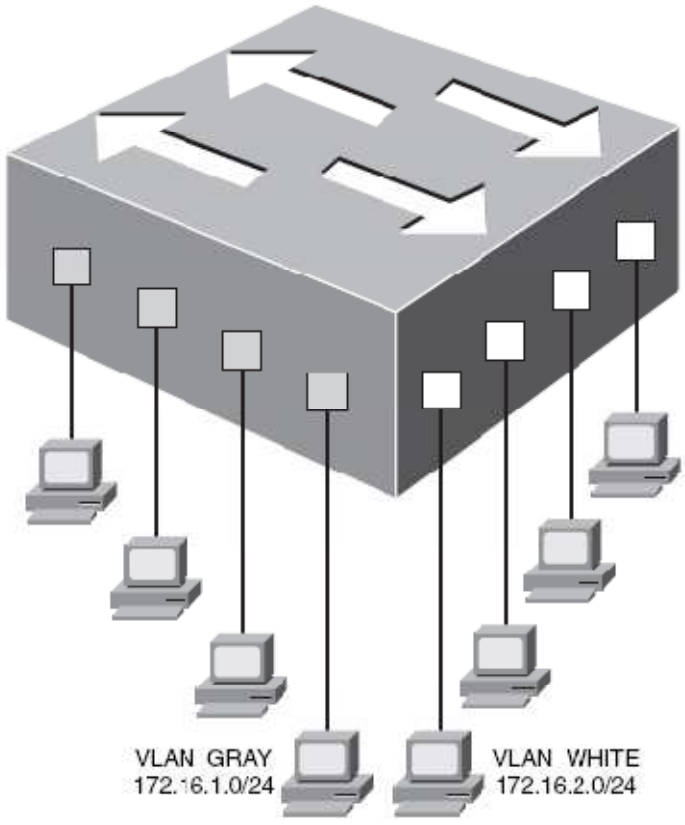


Figura 3.9 – Creación de VLAN

Fuente: http://biblioteca.utec.edu.sv/siab/virtual/tesis/55320.pdf

Los cuatro puertos en el lado izquierdo del switch están en la VLAN_GRAY y los cuatro puertos en el lado derecho están en la VLAN_WHITE, un cambio en esta configuración se puede ver como dos switches lógicos, imagínese teniendo el interruptor

de ocho puertos y romperse a la mitad (y de alguna manera las dos mitades del interruptor siguen funcionando).

Así es como VLAN son capaces de separar los dispositivos en el switch, si un dispositivo en VLAN_GRAY envía un mensaje, sólo llega a los dispositivos de VLAN_GRAY (esto es lo que se entiende por dominios de difusión separados).

Del mismo modo, los dispositivos en la VLAN separadas se asignan a las diferentes direcciones de subred IP, ya que son vistos como algo separado de redes lógicas. Sin una solución de enrutamiento (por medio de un router) en su lugar, los dispositivos de VLAN_GRAY no son capaces de comunicarse en absoluto con los dispositivos de VLAN_WHITE.

CAPÍTULO 4
DISEÑO METODOLÓGICO PARA INTEGRACIÓN DE LA CÁTEDRA LABORATORIO DE TELEMÁTICA

Para la integración de la cátedra Laboratorio de Telemática usaremos el método científico, el mismo que dividiremos en 3 partes:

- Formulación de un pensum en la cual se integra la cátedra Laboratorio de Telemática.
- Planificación del calendario académico para la cátedra Laboratorio de Telemática.
- Diseño de los Escenarios de las prácticas de laboratorio de acuerdo al pensum.

4.1. Formulación de un pensum en la cual se integra la cátedra Laboratorio de Telemática.

Para la creación de este pensum académico en donde se integrara la cátedra Laboratorio de Telemática nos basaremos en el nuevo pensum académico para la carrera de Ingeniería en Telecomunicaciones de la Facultad Técnica.

El objetivo principal de este laboratorio es poner en práctica y consolidar los conocimientos adquiridos en las materias Telemática I y Telemática II, por este motivo este laboratorio tendrá como pre-requisito haber aprobado la materia Telemática I y como co-requisito la materia Telemática II, es decir para poder cursar este laboratorio es necesario estar cursando Telemática II.

4.1.1. Número de Horas y Créditosal aprobar Laboratorio de Telemática.

La cátedra Laboratorio de Telemática se la integrará en el VIII ciclo, debido a que en este ciclo es donde el estudiante debió haber aprobado Telemática I y por ende estar cursando Telemática II.

La materia a integrar tendrá 48 horas semestrales, es decir 3 horas por semana en una sola sesión semanal en la cual se realizará diferentes actividades que se especificará en la planificación de la cátedra.

Esta materia será válida por 3 créditos.

Se considera que con esta cantidad de horas semestrales el estudiante podrá salir con unas excelentes bases en lo que respecta al área del networking, consolidando los conocimientos obtenidos en las materias Telemática I y Telemática II.

4.1.2. Vista del pensum académico actual.

A continuación tenemos el pensum actualde Ingeniería en Telecomunicaciones:

Tabla 4.1 Asignaturas correspondientes al I CICLO actual.

ASIGNATURAS	HORAS PENSUM	HORAS SEMANA	CRÉDITOS
FÍSICA I	80	5	4
CÁLCULO I	80	5	4
INFORMÁTICA I	64	4	3
QUÍMICA	48	3	3
FUNDAMENTOS DE INGENIERÍA	64	4	3
IDIOMA	64	4	3
TEOLOGÍA I	48	3	3
INGLÉS BÁSICO I	48	3	3
	496	31	26

Fuente:http://www2.ucsg.edu.ec/tecnica/index.php?option=com_content&view=article&id=60&itemid=101

Tabla 4.2 Asignaturas correspondientes al II CICLO actual.

ASIGNATURAS	HORAS PENSUM	HORAS SEMANA	CRÉDITOS
FÍSICA II	80	5	4
CÁLCULO II	80	5	4
INFORMÁTICA II	64	4	3
ALGEBRA LINEAL	48	3	3
CONTABILIDAD BÁSICA	64	4	3
TEOLOGÍA II	48	3	3
INGLÉS BASICO II	48	3	3
	432	27	23

Fuente:http://www2.ucsg.edu.ec/tecnica/index.php?option=com_content&view=article&id=60&itemid=101

Tabla 4.3 Asignaturas correspondientes al III CICLO actual.

ASIGNATURAS	HORAS PENSUM	HORAS SEMANA	CRÉDITOS
FÍSICA III	64	4	3
CÁLCULO III	64	4	3
INFORMÁTICA III	64	4	3
ANÁLISIS NUMÉRICO	64	4	3
CIRCUITOS ELÉCTRICOS I	80	5	4
MATEMÁTICAS FINANCIERAS	48	3	3
INTR. AL PENSAMIENTO CRÍTICO	48	3	3
INGLÉS BÁSICO III	48	3	3
	480	30	25

Fuente:http://www2.ucsg.edu.ec/tecnica/index.php?option=com_content&view=article&id=60&itemid=101

Tabla 4.4 Asignaturas correspondientes al IV CICLO actual.

ASIGNATURAS	HORAS PENSUM	HORAS SEMANA	CRÉDITOS
PROBABILIDADES Y ESTADÍSTICAS	64	4	3
CÁLCULO IV	64	4	3
FUNDAMENTOS DE MÉTODOS DE INVESTIGACIÓN	48	3	3
LABORATORIO DE CIRCUITOS	64	4	3
CIRCUITOS ELÉCTRICOS II	80	5	4
ELECTRÓNICA I	80	5	4
ESTUDIOS CONTEMPORÁNEOS	48	3	3
	448	28	23

Fuente:http://www2.ucsg.edu.ec/tecnica/index.php?option=com_content&view=article&id=60&itemid=101

Tabla 4.5 Asignaturas correspondientes al V CICLO actual.

ASIGNATURAS	HORAS PENSUM	HORAS SEMANA	CRÉDITOS
TEORÍA ELECTROMAGNÉTICA	64	4	3
SEÑALES Y SISTEMAS	48	3	3
PLANTA EXTERNA	64	4	3
DIGITALES I	80	5	4
LABORATORIO DE ELECTRÓNICA	64	4	3
ELECTRÓNICA II	80	5	4
ADMINISTRACIÓN DE RIESGOS	48	3	3
INGLÉS IV	48	3	3
	496	31	26

Fuente:http://www2.ucsg.edu.ec/tecnica/index.php?option=com_content&view=article&id=60&itemid=101

Tabla 4.6 Asignaturas correspondientes al VI CICLO actual.

ASIGNATURAS	HORAS PENSUM	HORAS SEMANA	CRÉDITOS
PROPAGACIÓN	64	4	3
FUNDAMENTOS DE COMUNICACIÓN	80	5	4
COMMUTACIÓN Y TRÁFICO TELEFÓNICO	48	3	3
DIGITALES II	80	5	4
LABORATORIO DE DIGITALES	64	4	3
MICROCONTROLADORES	64	4	3
ÉTICA	48	3	3
INGLÉS V	48	3	3
	496	31	26

Fuente:http://www2.ucsg.edu.ec/tecnica/index.php?option=com_content&view=article&id=60&itemid=101

Tabla 4.7 Asignaturas correspondientes al VII CICLO actual.

ASIGNATURAS	HORAS PENSUM	HORAS SEMANA	CRÉDITOS
TELEMÁTICA I	64	4	3
TRANSMISIÓN	64	4	3
PROCESAMIENTO DIGITAL DE SEÑALES	64	4	3
LÍNEAS DE TRANSMISIÓN	64	4	3
INVESTIGAC. OPERATIVA	80	5	4
ANTENAS	80	5	4
SISTEMA MICROPROCESADORES	48	3	3
	464	29	23

Fuente:http://www2.ucsg.edu.ec/tecnica/index.php?option=com_content&view=article&id=60&itemid=101

Tabla 4.8 Asignaturas correspondientes al VIII CICLO actual

ASIGNATURAS	HORAS PENSUM	HORAS SEMANA	CRÉDITOS
COMUNICACIONES INALÁMBRICAS	48	3	3
SISTEMAS SÍNCRONOS	64	4	3
SISTEMAS DE TELEVISIÓN	48	3	3
DISEÑO ELECTRÓNICO/DIGITAL	64	4	3
ECONOMÍA	64	4	3
SISTEMA FIBRA ÓPTICA	64	4	3
TELEMÁTICA II	64	4	3
	464	29	24

Fuente:http://www2.ucsg.edu.ec/tecnica/index.php?option=com_content&view=article&id=60&itemid=101

Tabla 4.9 Asignaturas correspondientes al IX CICLO actual.

ASIGNATURAS	HORAS PENSUM	HORAS SEMANA	CRÉDITOS
SISTEMAS DE COMUNICACIÓN	64	4	3
SISTEMAS SATELITÁLES	64	4	3
GESTIÓN DE LA RED	48	3	3
MARCO LEGAL DE TELECOMUNICACIONES	48	3	3
ESTUDIO IMPACTO AMBIENTAL	64	4	3
ANÁLISIS Y EVALUACIÓN PROYECTOS	80	5	4
ADMINISTRACIÓN DE EMPRESAS	64	4	3
	432	27	22

Fuente:http://www2.ucsg.edu.ec/tecnica/index.php?option=com_content&view=article&id=60&itemid=101

4.1.3. Vista del nuevo pensum académico.

A continuación se muestra como quedaría el nuevo pensum académico con la materia Laboratorio de Telemática dentro del VIII ciclo.

Tabla 4.10 Asignaturas correspondientes al I CICLO nuevo.

ASIGNATURAS	HORAS PENSUM	HORAS SEMANA	CRÉDITOS
FÍSICA I	80	5	4
CÁLCULO I	80	5	4
INFORMÁTICA I	64	4	3
QUÍMICA	48	3	3
FUNDAMENTOS DE INGENIERÍA	64	4	3
IDIOMA	64	4	3
TEOLOGÍA I	48	3	3
INGLÉS BÁSICO I	48	3	3
	496	31	26

Fuente:http://www2.ucsg.edu.ec/tecnica/index.php?option=com_content&view=article&id=60&itemid=101

Tabla 4.11 Asignaturas correspondientes al II CICLO nuevo.

ASIGNATURAS	HORAS PENSUM	HORAS SEMANA	CRÉDITOS
FÍSICA II	80	5	4
CÁLCULO II	80	5	4
INFORMÁTICA II	64	4	3
ALGEBRA LINEAL	48	3	3
CONTABILIDAD BÁSICA	64	4	3
TEOLOGÍA II	48	3	3
INGLÉS BASICO II	48	3	3
	432	27	23

Fuente:http://www2.ucsg.edu.ec/tecnica/index.php?option=com_content&view=article&id=60&itemid=101

Tabla 4.12 Asignaturas correspondientes al III CICLO nuevo.

ASIGNATURAS	HORAS PENSUM	HORAS SEMANA	CRÉDITOS
FÍSICA III	64	4	3
CÁLCULO III	64	4	3
INFORMÁTICA III	64	4	3
ANÁLISIS NUMÉRICO	64	4	3
CIRCUITOS ELÉCTRICOS I	80	5	4
MATEMÁTICAS FINANCIERAS	48	3	3
INTR. AL PENSAMIENTO CRÍTICO	48	3	3
INGLÉS BÁSICO III	48	3	3
	480	30	25

Fuente:http://www2.ucsg.edu.ec/tecnica/index.php?option=com_content&view=article&id=60&itemid=101

Tabla 4.13 Asignaturas correspondientes al IV CICLOnuevo.

ASIGNATURAS	HORAS PENSUM	HORAS SEMANA	CRÉDITOS
PROBABILIDADES Y ESTADÍSTICAS	64	4	3
CÁLCULO IV	64	4	3
FUNDAMENTOS DE MÉTODOS DE INVESTIGACIÓN	48	3	3
LABORATORIO DE CIRCUITOS	64	4	3
CIRCUITOS ELÉCTRICOS II	80	5	4
ELECTRÓNICA I	80	5	4
ESTUDIOS CONTEMPORÁNEOS	48	3	3
	448	28	23

Fuente:http://www2.ucsg.edu.ec/tecnica/index.php?option=com_content&view=article&id=60&itemid=101

Tabla 4.14 Asignaturas correspondientes al V CICLOnuevo.

ASIGNATURAS	HORAS PENSUM	HORAS SEMANA	CRÉDITOS
TEORÍA ELECTROMAGNÉTICA	64	4	3
SEÑALES Y SISTEMAS	48	3	3
PLANTA EXTERNA	64	4	3
DIGITALES I	80	5	4
LABORATORIO DE ELECTRÓNICA	64	4	3
ELECTRÓNICA II	80	5	4
ADMINISTRACIÓN DE RIESGOS	48	3	3
INGLÉS IV	48	3	3
	496	31	26

Fuente:http://www2.ucsg.edu.ec/tecnica/index.php?option=com_content&view=article&id=60&itemid=101

Tabla 4.15 Asignaturas correspondientes al VI CICLOnuevo.

ASIGNATURAS	HORAS PENSUM	HORAS SEMANA	CRÉDITOS
PROPAGACIÓN	64	4	3
FUNDAMENTOS DE COMUNICACIÓN	80	5	4
COMMUTACIÓN Y TRÁFICO TELEFÓNICO	48	3	3
DIGITALES II	80	5	4
LABORATORIO DE DIGITALES	64	4	3
MICROCONTROLADORES	64	4	3
ÉTICA	48	3	3
INGLÉS V	48	3	3
	496	31	26

Fuente:http://www2.ucsg.edu.ec/tecnica/index.php?option=com_content&view=article&id=60&itemid=101

Tabla 4.16 Asignaturas correspondientes al VII CICLOnuevo.

ASIGNATURAS	HORAS PENSUM	HORAS SEMANA	CRÉDITOS
TELEMÁTICA I	64	4	3
TRANSMISIÓN	64	4	3
PROCESAMIENTO DIGITAL DE SEÑALES	64	4	3
LÍNEAS DE TRANSMISIÓN	64	4	3
INVESTIGAC. OPERATIVA	80	5	4
ANTENAS	80	5	4
SISTEMA MICROPROCESADORES	48	3	3
	464	29	23

Fuente:http://www2.ucsg.edu.ec/tecnica/index.php?option=com_content&view=article&id=60&itemid=101

Tabla 4.17 Asignaturas correspondientes al VIII CICLO donde se integrará la materia Laboratorio de Telemática

ASIGNATURAS	HORAS PENSUM	HORAS SEMANA	CRÉDITOS
COMUNICACIONES INALÁMBRICAS	48	3	3
SISTEMAS SÍNCRONOS	64	4	3
SISTEMAS DE TELEVISIÓN	48	3	3
DISEÑO ELECTRÓNICO/DIGITAL	64	4	3
ECONOMÍA	64	4	3
SISTEMA FIBRA ÓPTICA	64	4	3
TELEMÁTICA II	64	4	3
LABORATORIO DE TELEMÁTICA	**48**	**3**	**3**
	464	29	24

Fuente: los autores

Tabla 4.18 Asignaturas correspondientes al IX CICLO nuevo.

ASIGNATURAS	HORAS PENSUM	HORAS SEMANA	CRÉDITOS
SISTEMAS DE COMUNICACIÓN	64	4	3
SISTEMAS SATELITÁLES	64	4	3
GESTIÓN DE LA RED	48	3	3
MARCO LEGAL DE TELECOMUNICACIONES	48	3	3
ESTUDIO IMPACTO AMBIENTAL	64	4	3
ANÁLISIS Y EVALUACIÓN PROYECTOS	80	5	4
ADMINISTRACIÓN DE EMPRESAS	64	4	3
	432	27	22

Fuente:http://www2.ucsg.edu.ec/tecnica/index.php?option=com_content&view=article&id=60&itemid=101

4.2. Planificación del calendario académico para la cátedra Laboratorio de Telemática.

En esta sección se describirá una breve planificación de que es lo que se realizará durante un semestre regular, teniendo en cuenta que un semestre regular son 16 semanas de clases y que cada clase de Laboratorio de Telemática será de 3 horas, una sesión por semana.

Antes de cada práctica se tomará una lección de 10 minutos para evaluar si los estudiantes vienen preparados previos a la práctica correspondiente.

Los estudiantes deberán presentar un reporte de la práctica anterior, respondiendo unas preguntas formuladas por el profesor del curso, con esto se puede evaluar el rendimiento de los estudiantes cada práctica.

Al final del curso los estudiantes deberán presentar un proyecto relacionado con el laboratorio de telemática utilizando el simulador GNS3; el tema lo deberán escoger los estudiantes y este debe ser presentado y aprobado por el profesor hasta antes de la 4ta semana de clases, caso contrario dicho proyecto se irá devaluando en puntaje correspondiente.

4.2.1. Ponderación del puntaje correspondiente a la materia Laboratorio de Telemática.

El Laboratorio de Telemáticaserá ponderado de una forma equitativa y de acuerdo a las responsabilidades que se les asignen a los estudiantes, para la ponderación de la materia se tomará en cuenta la asistencia de los estudiantes al curso, visto de manera justa y basándose en metodologías de laboratorios de otras universidades la forma de ponderación será la siguiente:

- Asistencia 10 puntos
- Lecciones 20 puntos
- Reportes 20 puntos
- Proyecto 50 puntos

Sumando un total del 100 puntos.

Dentro del porcentaje de ponderación correspondiente al proyecto se evaluará también los avances correspondientes al mismo, esto quedara a criterio del profesor de la cátedra

4.2.2. Calendario de actividades de la materia Laboratorio de Telemática.

A continuación se muestra un calendario de actividades de la materia Laboratorio de Telemática, cabe recalcar que para esta materia, mostraremos un total de 8 escenarios para prácticas del laboratorio más adelante, por lo tanto en este laboratorio tendrá un equivalente de 8 practicas por semestre.

Tabla 4.19 Calendario de actividades de la materia Laboratorio de Telemática durante un semestre regular

SEMANA 1	PRESENTACION Y POLITICAS DEL CURSO
SEMANA 2	INTRODUCCION Y TEORIA CORRESPONDIENTE AL SIMULADOR GNS3 Y DEMAS HERRAMIENTAS A USAR EN EL LABORATORIO DE TELEMATICA
SEMANA 3	PRACTICA #1
SEMANA 4	PRACTICA #2
SEMANA 5	PRESENTACION Y APOBRACION DEL TEMA DE PROYECTO
SEMANA 6	PRACTICA #3
SEMANA 7	PRACTICA #4
SEMANA 8	EXAMENES 1ER PARCIAL
SEMANA 9	PRESENTACION DE AVANCE DE PROYECTO
SEMANA 10	PRACTICA #5
SEMANA 11	PRACTICA #6
SEMANA 12	PRACTICA #7
SEMANA 13	PRACTICA #8
SEMANA 14	LIBRE
SEMANA 15	PRESENTACION FINAL DEL PROYECTO
SEMANA 16	EXAMENES FINALES

Fuente: los autores

4.3. Diseño de los escenarios de las prácticas de laboratorio de acuerdo a la planificación de la materia.

De acuerdo a la planificación de la materia que se desea integrar en la Facultad Técnica, se mostraran 8 escenarios los cuales corresponderán a las 8 prácticas propuestas en el calendario de actividades de la materia, basándose cada una de estas en los conocimientos obtenidos en la materia Telemática I y lo correspondiente al material que se estudiará en la materia Telemática II.

A continuación se mostraran uno a uno los escenarios para la creación de prácticas del nuevo laboratorio de telemática.

Nota: Cabe recalcar que este proyecto es sumamente investigativo por lo cual no es ha invertido en la compra de los routers Cisco y demás equipos físicos a utilizar en la implementación de cada una de las practicas por lo que se ha decidido crear escenarios basándonos en posibles resultados obtenidos en base a nuestros conocimientos de networking y además de ayudas de prácticas ya realizadas anteriormente en otros laboratorios de Universidades de gran prestigio.

De igual forma en la sección de ANEXOS se describirá los comandos más importantes para la implementación de cada uno de estos escenarios y así poder completar la integración de la materia laboratorio de Telemática con sus respectivas prácticas ya diseñadas para la enseñanza a los estudiantes.

4.3.1. Escenario 1: Conexión de 3 routers Cisco con GNS3

En este escenario se comprobará el funcionamiento más básico de GNS3, por lo tanto en la primera toma de contacto se diseñará una red con 3 routers Cisco 7200 conectados como se puede ver en la figura 4.1

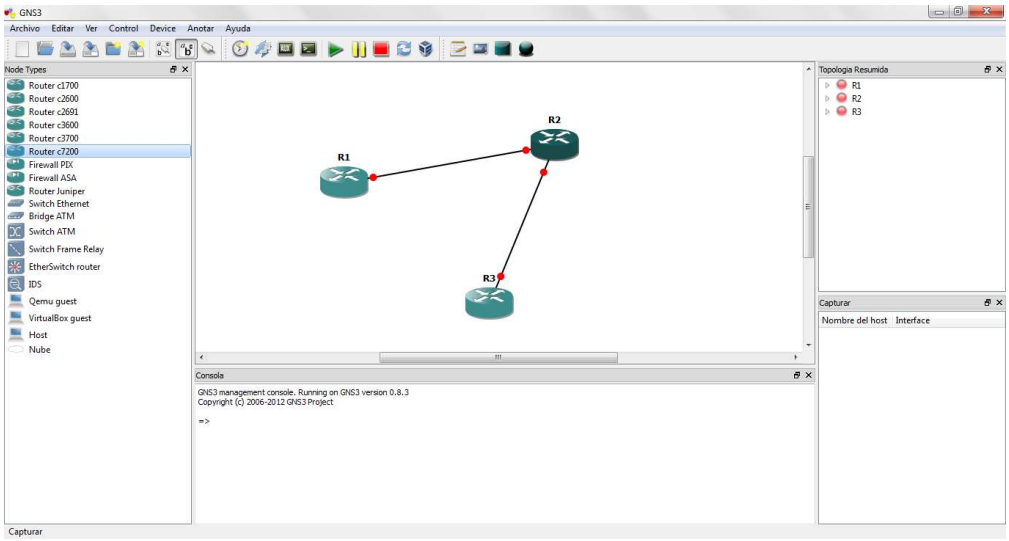


Figura 4.1 – Red de 3 routers Cisco en GNS3

Fuente: los autores (Simulador GNS3)

En este ensayo realizado con GNS3, además de la primera toma de contacto con laaplicación GNS3, también se comprobará la conectividad entre los *routers*. Fijándose en la Figura 3.1, se observa que en el centro de la imagen permanece configurada la red quese desea analizar. Se puede evidenciar que una persona que no tenga los conocimientosnecesarios puede crear dicho escenario. Si uno se fija en la parte izquierda de la Figura 3.1 comprueba la disposición de todos los elementos que se pueden utilizar para lacreación de nuevos escenarios, estos elementos se usarán en escenarios futuros.

Fijándose de igual forma en la parte de abajo se comprueba que ésta es la antiguaconsola de Dynagen. Como consecuencia ya no será necesario cargar el servidor deDynamips, éste ya será ejecutado de forma automática a la vez que inicia la aplicaciónde GNS3.

Como podemos observar en la figura 4.2 la forma de diseñar este escenario utilizando GNS3 es muy fácil y sencillo ya que se pueden cargar las consolas de los routers o simplemente activarlos.(Anuzelli)

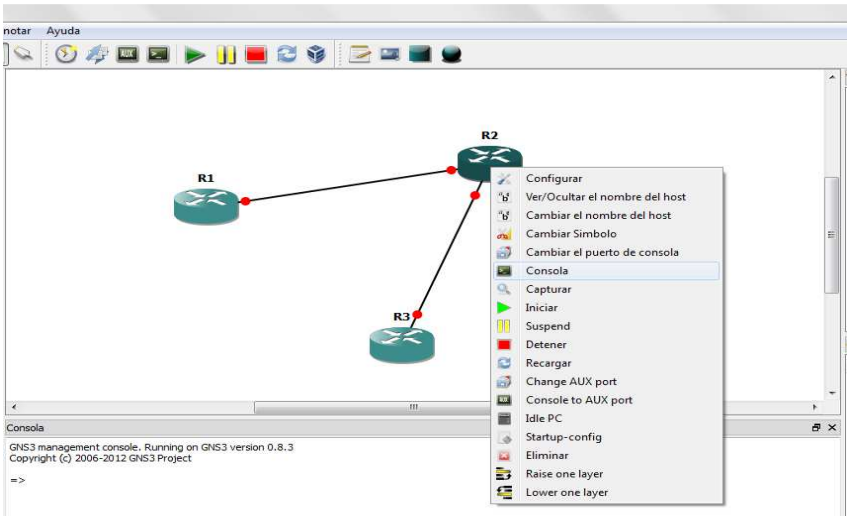


Figura 4.2 – Opciones de los routers en GNS3

Fuente: los autores (Simulador GNS3)

También se descubre cómo se solucionan problemas tan sencillos como cambiar elnombre, configurarlo, iniciarlo, pararlo, etc.

También se puede destacar que en este caso la asignación de las interfaces Ethernet sepodrán hacer de forma automática o de forma manual (Figura 4.3).

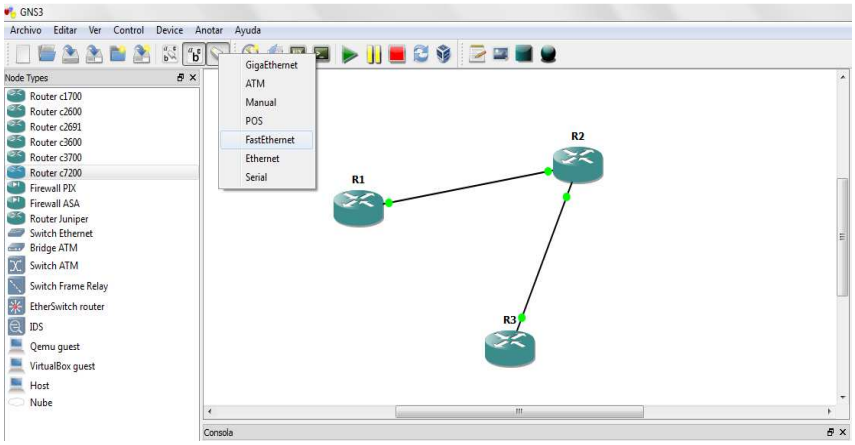


Figura 4.3 – Creación de Interfaces

Fuente: los autores (Simulador GNS3)

Con la interfaz gráfica se obtiene mayor cantidad de información, así como una mayor facilidad de creación de escenarios.

Una vez inicializados los *routers*para su configuración habrá que seguir los mismos pasos indicados en los escenarios ya expuestos en apartados anteriores. En los futuros escenarios siempre se seguirá esta forma de trabajo.

Cuando los routersestán puestos en marcha y configurados, lo único que hay que hacer es ver cómo se comunican entre sí, pudiendo así concluir y analizar con respecto al funcionamiento de los dispositivos en cada uno de los escenarios.

En los siguientes escenarios estos pasos ya no se mostrarán, debido a que siempre se realizará de la misma manera, por lo tanto cuando se hable de que se inicia la máquina o que se para, se podrá hacer tanto gráficamente como por medio de la consola. Como se ha indicado ya, en los futuros escenarios también se le podrán poner conmutadores, redes, así como todas aquellas opciones que proporciona la interfaz gráfica.

4.3.2. Escenario 2: Conexión de equipos reales con GNS3

Para este escenario, se creará directamente una interfaz entre el *router*y la tarjeta de red, sin la necesidad de un conmutador intermedio, observando en la interfaz gráfica como quedaría (Figura 4.4). Hay que tener en cuenta que los nombres de los *routers*seguirán siendo los mismos que se indicaron.

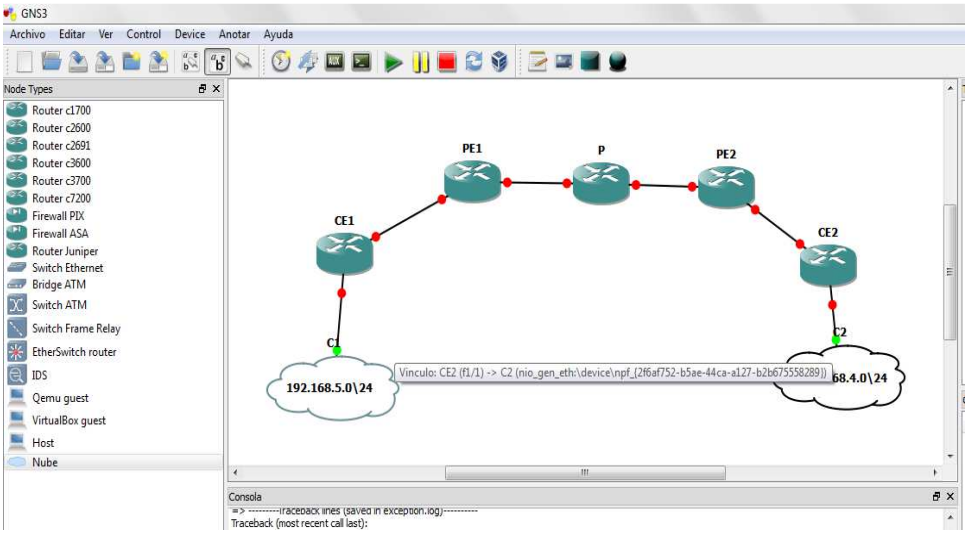


Figura 4.4 – Escenario a realizar por GNS3

Fuente: los autores (Simulador GNS3)

Se puede ver que para crear las interfaces lo primero que hay que hacer es crear redes. Como van a ser de carácter privado se pueden poner redes con tantas direcciones como se desee, por lo que se pondrá una máscara lo suficientemente grande como para conectar más de un ordenador en un futuro. Por lo tanto el PC1 pertenecerá a la red 192.168.5.0 /24 y el PC2 pertenecerá a la red 192.168.4.0 /24. Hay que destacar la forma en la que se asignan las direcciones (Figura 4.5).

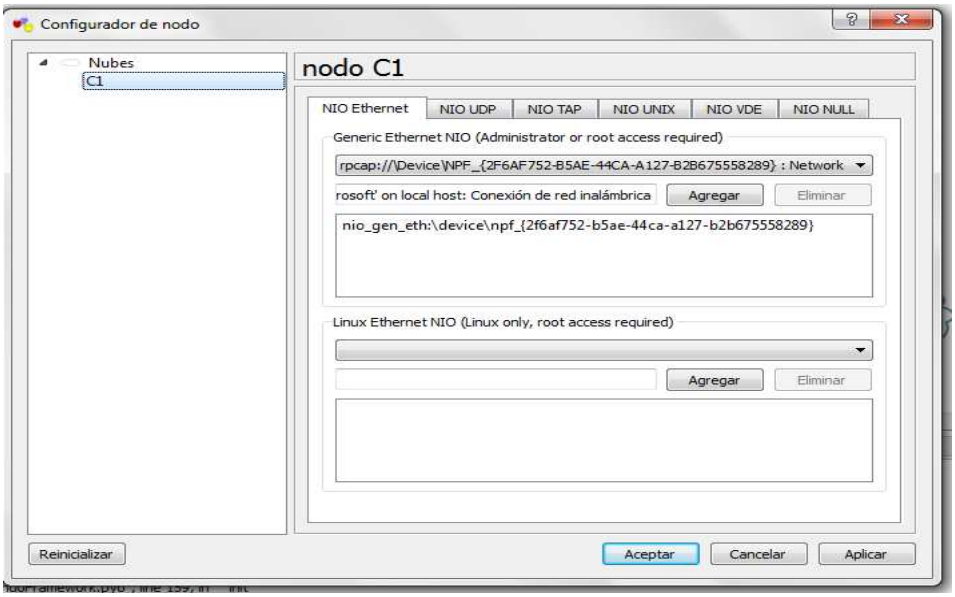


Figura 4.5 – Asignación de tarjetas de red

Fuente: los autores (Simulador GNS3)

4.3.3. Escenario 3: Conectividad entre routers reales y simulados

En este escenario se va a demostrar la conectividad de los *routers*Cisco simuladoscon *routers*reales y también se verán las posibilidades y capacidades que aportará lainterfaz gráfica, así como todo el potencial de Dynagen/Dynamips. En la Figura 4.6 semuestra el escenario que se va a realizar en la interfaz gráfica.

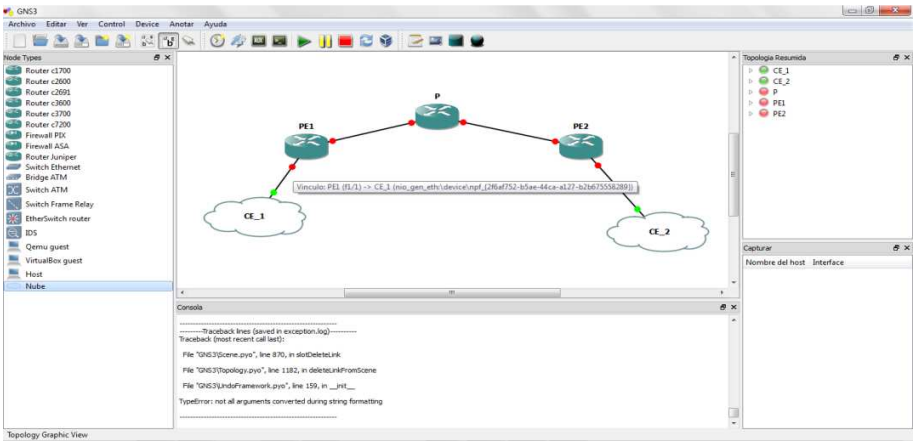


Figura 4.6 – Red creada en GNS3

Fuente: los autores (Simulador GNS3)

Como se puede observar en este caso, se han vuelto a utilizar las mismas tarjetas de red, pero en esta ocasión éstas estarán conectadas directamente al *router*Atlas, cabe recalcar que el router Atlas al que se hace referencia es un dispositivo físico, por lo que a continuación en la figura 4.7 se muestra el escenario completo de cómo quedaría nuestra red. Para lograrlo se ha tenido que cambiar la configuración del conmutador. En este escenario los puertos que se utilizaban para conectar a los ordenadores se sustituyen para conectar a los *routers*Atlas, por lo que se crean otras dos VLAN (ver figura 4.7).

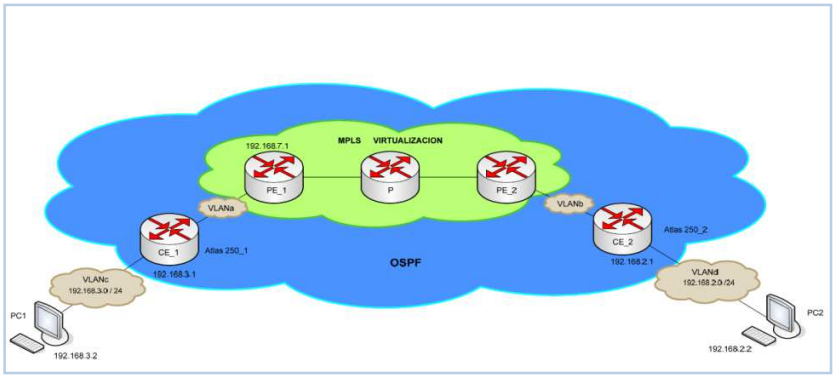


Figura 4.7 – Escenario completo de la red diseñada

Fuente: http://es.scribd.com/doc/75286465/VlAN

Hay que tener en cuenta que tanto los *routers*Atlas como los ordenadores son elementos reales y no virtuales como sucede con las VM o las redes creadas con GNS3, por lo tanto la interfaz que conecta a los *routers*Cisco simulados y a los *routers*Atlas será una interfaz física la cual tendrán que compartir un mismo protocolo de encaminamiento *OSPF*.

En este caso, los *routers*Atlas funcionaran como "CE" y los *routers*simulados actuarán como "PE" y "P", tal y como se puede comprobar en la Figura 4.7. Ahora será interesante mostrar la conectividad existente entre ambos extremos, con lo que también se comprueban los problemas comentados referentes a los retardos existentes al enviar los paquetes. En la figura 4.8 se muestra como sería la conectividad entre ambos ordenadores.

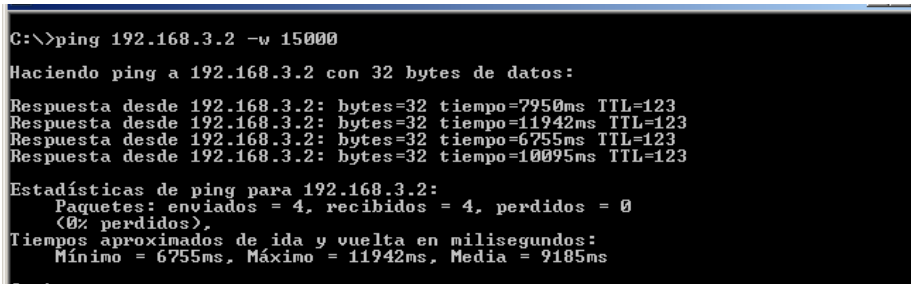


Figura 4.8 – Realización de ping desde PC2 a PC1

Fuente: http://es.scribd.com/doc/75286465/VlAN

4.3.4. Escenario 4: Interacción entre diferentes VM

En este escenario se pretende indicar la posibilidad de conectar más máquinas almismo escenario visto anteriormente (Figura 4.7). Para ello se va a comprobar laposibilidad de conectar redes entre diferentes VM existentes, para lo cual se necesitarándos tarjetas de red virtuales. Una de ellas se conectará a la VM existente para lacreación de los escenarios y la otra tarjeta de red se utilizará para configurarla en otraVM que se utiliza como *Web Server*.

Una vez configurada correctamente la interfaz que conecta al *WebServer*(ver Anexo II), se demuestra que la conectividad entre ambas VM es total. En este escenariose llega al límite de tarjetas Ethernet con las que se puede trabajar, por lo que en losfuturos escenarios que se realicen, no se podrán poner más tarjetas de red.

Se podrá observar en la Figura 4.9 que se ha utilizado un mismo *router*Cisco “PE2”para conectar dos redes distintas, por lo que se mostrará una alternativa donde cada*router*Cisco “PE” tenga su propia interfaz de salida.

Se necesitará hacer un ping desde cualquiera de losequipos hasta el *Web Server*. La dirección del servidor está indicada en la Figura 4.10.

Igualmente se tendrá en cuenta el tiempo que tardan enllegar los paquetes.

En la figura 4.9 se muestran los escenarios comentados, cabe destacar que en estosescenarios ya no se indicarán los protocolos a utilizar, esto es debido a que ya seexplicaron los protocolos de encaminamiento utilizados *OSPF* y *MPLS*. Además, enestos escenarios no sólo se van a detallar las redes o *router*sa utilizar, sino que tambiénse mostrarán las direcciones *IP* utilizadas en los ensayos.

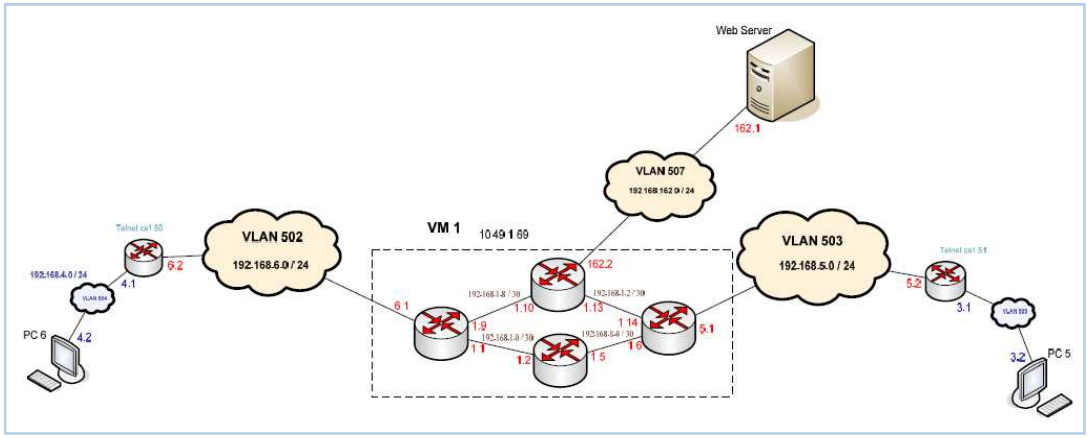


Figura 4.9 – Conexión con WebServer

Fuente: http://es.scribd.com/doc/75286465/VlAN

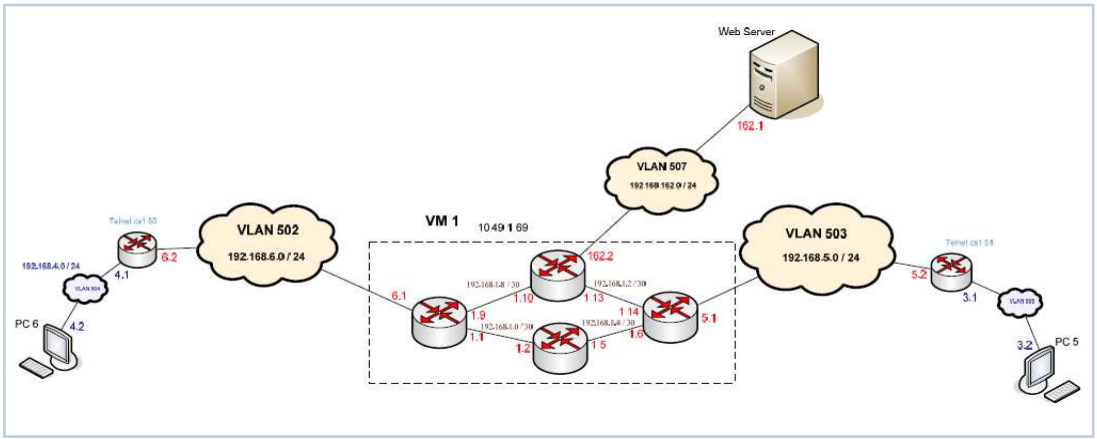


Figura 4.10 – Escenario alternativo con otro router Cisco “PE”

Fuente: http://es.scribd.com/doc/75286465/VlAN

4.3.5. Escenario 5: Conexión con 802.1Q

802.1Q también conocida como dot1q,es una arquitectura de encapsulado que resuelve el problemade compartir un mismo medio físico entre varias redes de forma transparente.

En este escenario se van a intentar solucionar los problemas relacionados con laslimitaciones existentes con las tarjetas de red. Con este ensayo además se van a poderanalizar otros aspectos de interés, como el posible cuello de botella que se crea cuandoen una misma tarjeta de red se configuran varias interfaces y conjuntamente comprobarlas consecuencias de utilizar interfaces etiquetadas.

Se pretende demostrar con este experimento que, pese a no soportar VMware lacreación de interfaces de red virtuales mediante la aplicación de 802.1Q, si es posiblecrear estas interfaces en los routersde Dynagen/Dynamips, siendo VMware transparente a las tramas etiquetadas.

Como se puede observar en la Figura 4.11, se van a mantener los mismos elementosque en el escenario 4. De esta manera se va a llegar al límite de tarjetas de red que puede proporcionar VMWare.

Ahora se pretende descubrir cuál es el comportamiento no sólo de VMWare conrespecto a la creación de interfaces de red 802.1Q, sino también el comportamiento dela GNS3 y el producido en la red.(Martin, 2008)

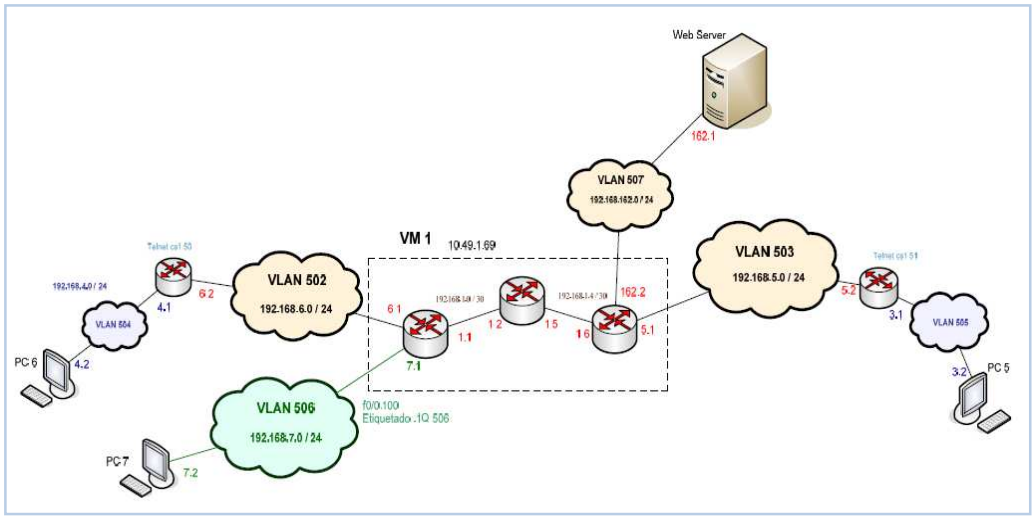


Figura 4.11 – VLAN .1Q “506”

Fuente: http://es.scribd.com/doc/75286465/VlAN

Para realizar estas pruebas, se debe utilizar una misma tarjeta de red tal y como se muestra en la Figura 4.12

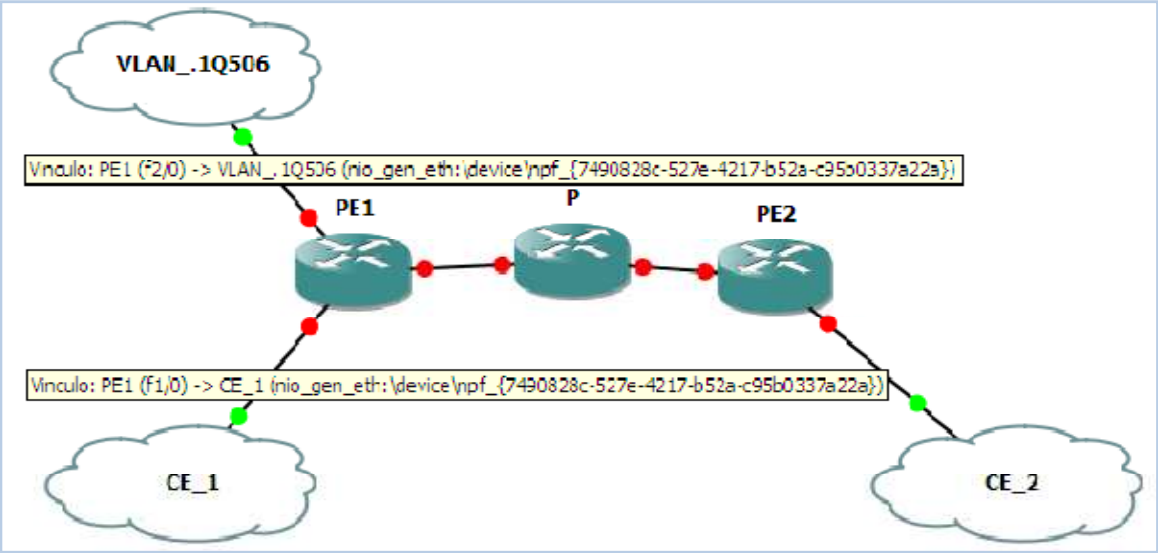


Figura 4.12 – Interfaz etiquetada .1Q 506 en GNS3

Fuente: los autores (Simulador GNS3)

Lo que se consigue internamente es utilizar la misma tarjeta de red, pero por la interfaz fastEthernet1/0 irá sin etiquetar y por la otra interfaz fastEthernet2/0 irá etiquetado con la etiqueta “506”. (Puede verse la configuración de la interfaz etiquetada en el ANEXO III).

Hay que tener en cuenta varios puntos, el más importante es que la interfaz física compartida en el conmutador gestionable será f0/0 y f0/0.100, pero como se ha podido observar en la Figura 4.12, en *GNS3* estas interfaces estarán diferenciadas en f1/0 y f2/0.

Otro punto a tener en cuenta es que en el conmutador se tendrá que crear otra VLAN, siendo ésta etiquetada con 802.*1Q* y su correspondiente etiqueta “506”, con lo que se consigue conectar el PC7 con el *router*Cisco “PE1”.

La consecuencia que se saca es que la tarjeta de red Ethernet virtual ni encapsula ni desencapsúla, lo único que hace es enviar la información tal y como le llega, siendo el *router*Cisco “PE1” y el conmutador configurable los que realizan las funciones de encapsular y desencapsular.

Una vez configurada correctamente la interfaz a encapsular se logra una conectividad entre todos los elementos de la red. Si se realiza una prueba desde cualquiera de los PCs hasta el PC7 conectado a la interfaz etiquetada, se demuestra que no afecta a su

comportamiento y su funcionamiento es igual al que se puede ver en la otra tarjeta de red, (ver figura 4.13).

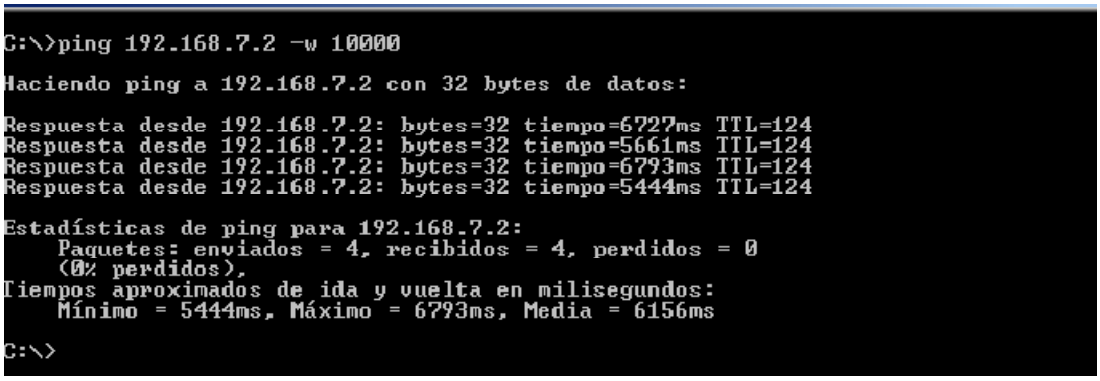


Figura 4.13 – Ping desde PC6 a PC7

Fuente: http://es.scribd.com/doc/75286465/VlAN

Se comprueba entonces que el uso de las interfaces etiquetadas no afecta a las tarjetas de red virtuales tal y como se observa en la Figura 4.13.

Para tener un concepto más claro de cómo se comporta el conmutador configurable con las tarjetas de red físicas y del mismo modo ver el comportamiento de la tarjeta de red virtualizada, se mostrará la siguiente Figura.

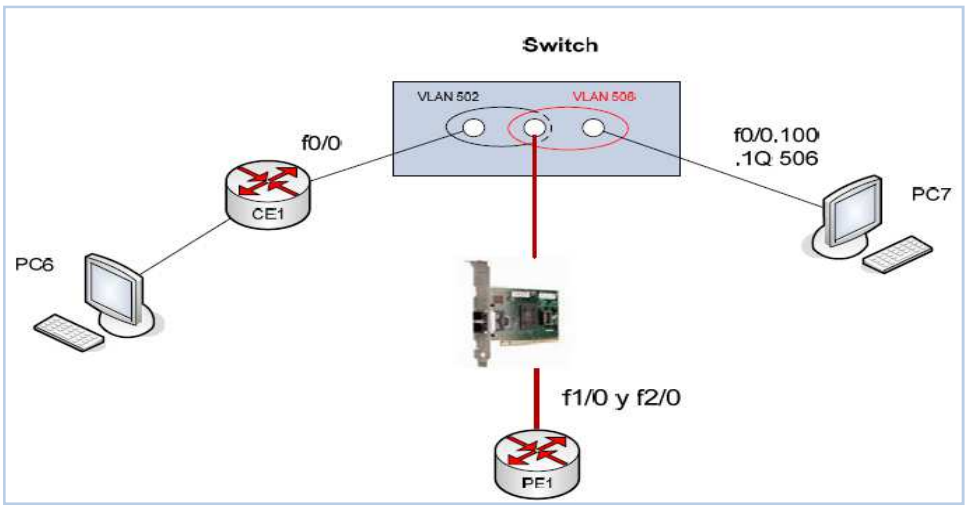


Figura 4.14 – Conexión en el Switch

Fuente: http://es.scribd.com/doc/75286465/VlAN

Con esta prueba se demuestran las limitaciones que se producen en la herramienta VMWare con respecto a las tarjetas de red Ethernet que se pueden utilizar en cada VM quedan solventadas. Hay que tener en cuenta que a la hora de crear los escenarios en

GNS3 no habrá diferencia si la interfaz a crear se va a etiquetar o no, ya que como se observa, se crean dos interfaces f1/0 y f2/0 y ambas pasan por la tarjeta de red sin que exista ninguna diferenciación. Por tanto se deduce que VMWare es totalmente transparente al etiquetado. El problema del etiquetado lo tendrá que resolver el *router*Cisco con su configuración.

Con lo que se ha aportado en este escenario y en los anteriores ya se tienen los conocimientos necesarios sobre las herramientas de *GNS3* y Dynagen/Dynamips. Estos conocimientos se utilizarán para plantear escenarios más complejos con los que se puedan trabajar pensando en la formación de los futuros ingenieros y que salgan con bases muy solidas con respecto al networking.

Nota: Para la realización de las prácticas futuras basándose en los escenarios investigativos que se presentaran a continuación se necesitarían más ordenadores así como nuevas VM en el servidor, lo que implicaría un costo adicional para la implementación de estas prácticas, y esto es un tema de discusión entre los miembros directivos de la Facultad Técnica, ya que son ellos quienes tomarían la decisión final con respecto a la inversión de esta cátedra.

4.3.6. Escenario 6: Creación de VPN

En este escenario, después de verificar que lo desarrollado en los apartadosanteriores funcionaba correctamente, se implementarán en un único escenario lodesarrollado hasta ahora, pudiendo experimentar a la vez con la posibilidad de crearVPN.

La única diferencia que se va a realizar en esta prueba es que en vez de utilizar lainterfaz de la VM del *Web Server* se usará otra que conectará a una VM diferente dondese creará otro escenario, por lo tanto en este ensayo además de unir varias VM tambiénse unirán diferentes redes, como se puede comprobar en la Figura 4.15.

Como se ha realizado hasta el momento, lo primero que se llevará a cabo es laconexión de todos los equipos de la red tal y como se puede ver en la Figura 4.15, para lo cual se crearán diferentes *VLAN*.

Después de que se han creado todas las interfaces necesarias, se utilizará un mismoprotocolo de encaminamiento "*OSPF*" para comprobar que realmente existeconectividad entre todos los puntos de la red. Posteriormente se configurará en todos los*routers*Cisco simulados el protocolo de encaminamiento "*MPLS*" y así se estará endisposición de crear diferentes *VPN*.

En este ensayo se crearán dos *VPN*, la *VPN-A* y la *VPN-B* (ver Anexo IV), la *VPN-A*estará formada por los equipos PC5 y PC4, mientras que a la *VPN-B* estará formadapor los equipos PC7, PC6 y PC3.

Para realizar diferentes experimentos, los *routers*Cisco que pertenecen a la VM1estarán conectados directamente a los PCs sin la necesidad de tener un *router*intermedio, de esta manera se comprobarán los distintos comportamientos a los que estásometido *GNS3*.

Hay que tener en cuenta que el que estén corriendo dos máquinas virtuales en elservidor hace que éste tenga que repartir los recursos. Por tanto se tendrá en cuenta a lahora de realizar las ensayos de conectividad, sobre todo cuando se intente demostrar laconectividad entre ordenadores que tengan que a travesar mayor número de redes.(Martin, 2008)

A continuación se muestra el escenario completo para la creación de las VPN.

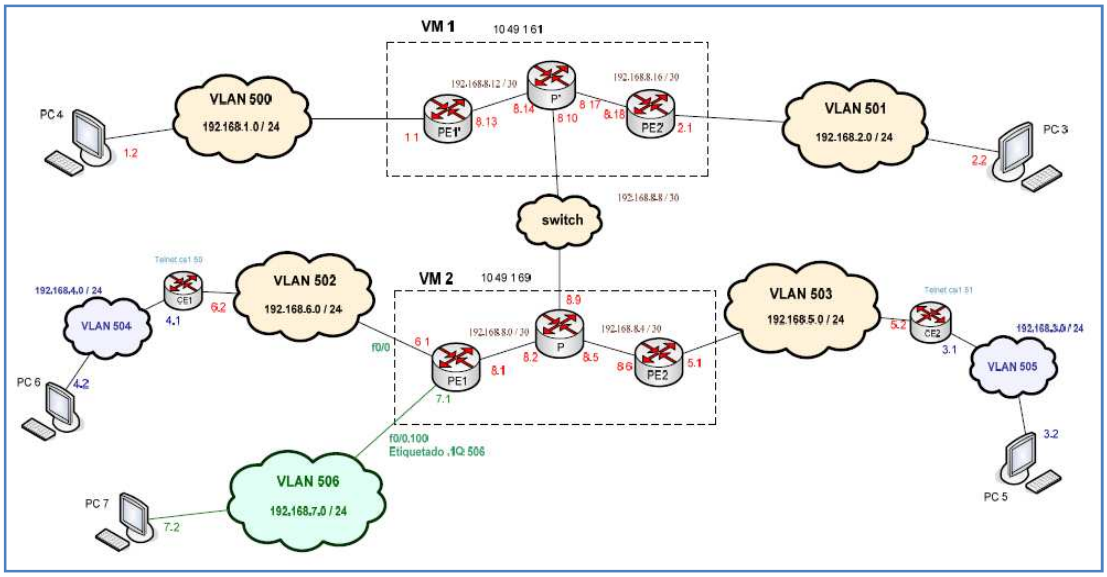


Figura 4.15 – Escenario para crear VPN

Fuente: http://es.scribd.com/doc/75286465/VlAN

Con esta distribución los PCs 6 y 7 se podrán comunicar con el PC3 y por otro lado el PC5 se podrá comunicar con el PC4, pero no así entre los demás. Para entender mejor este escenario se va a detallar el diseño realizado en la aplicación de *GNS3* (Figura 4.16 y Figura 4.17).

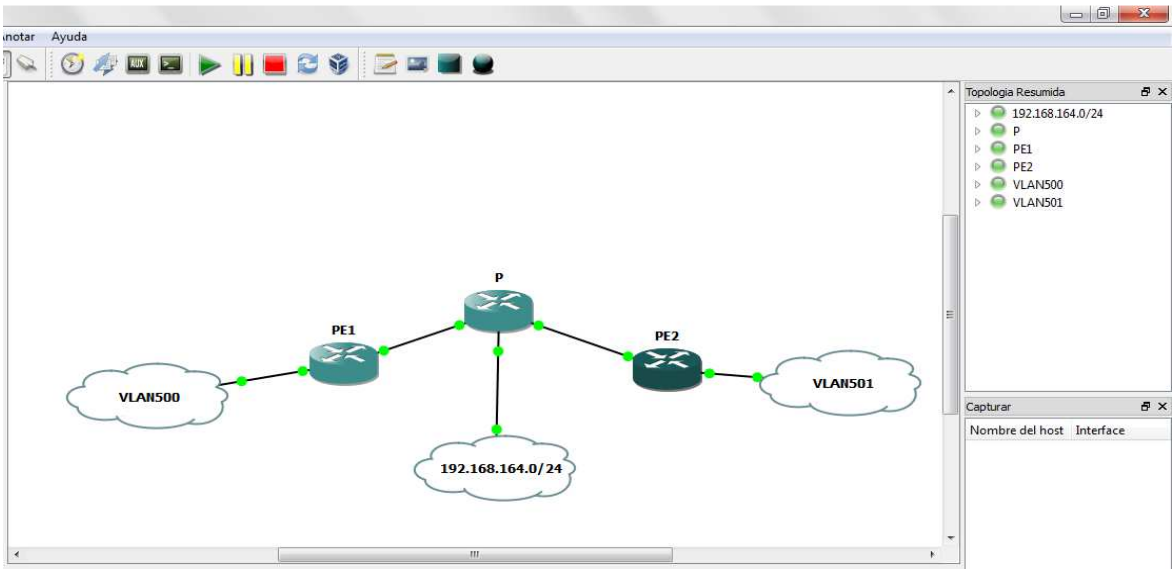


Figura 4.16 – Escenario creado en la VM1

Fuente: los autores (Simulador GNS3)

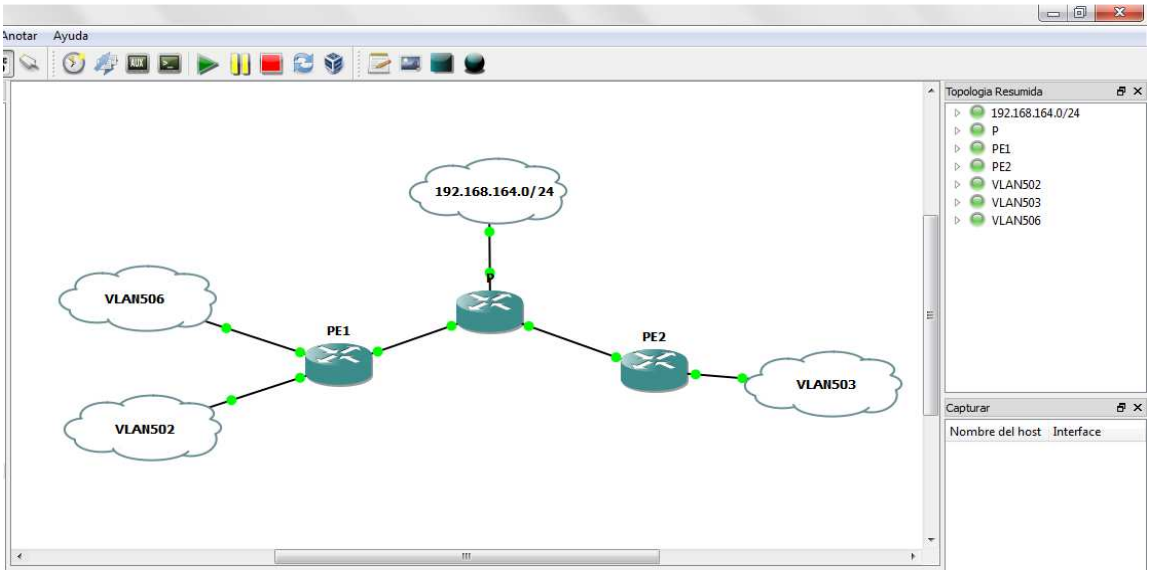


Figura 4.17 – Escenario creado en la VM2

Fuente: Simulador GNS3

Una vez especificada la red completa, se mostrarán los resultados obtenidos. Estosresultados contarán con la conectividad entre los PCs mediante el comando ping.Y por último se deben mostrarán las capturas realizadas desde la herramienta de *Wireshark*.

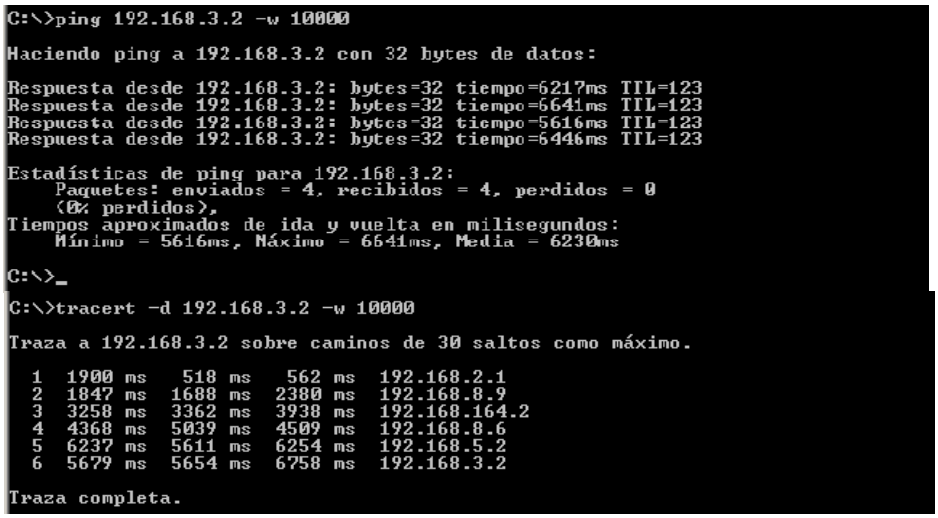


Figura 4.18 –Resultado de Ping y Traceroute desde PC3 al PC5

Fuente: http://es.scribd.com/doc/75286465/VlAN

Figura 4.19 – Resultado de Ping y Traceroute desde PC3 al PC7

Fuente: http://es.scribd.com/doc/75286465/VlAN

Se observa que el protocolo de encaminamiento con el que se están haciendo laspruebas es el protocolo OSPF, ya que por el contrario no debería poder llegar al PC5. Con estaspruebas se comprueba la conectividad existente entre distintas VM, además dedemostrar que hay comunicación a través de los enlaces etiquetados. Se puede destacarque accediendo tanto a enlaces etiquetados como sin etiquetar el tiempo de respuesta essimilar.

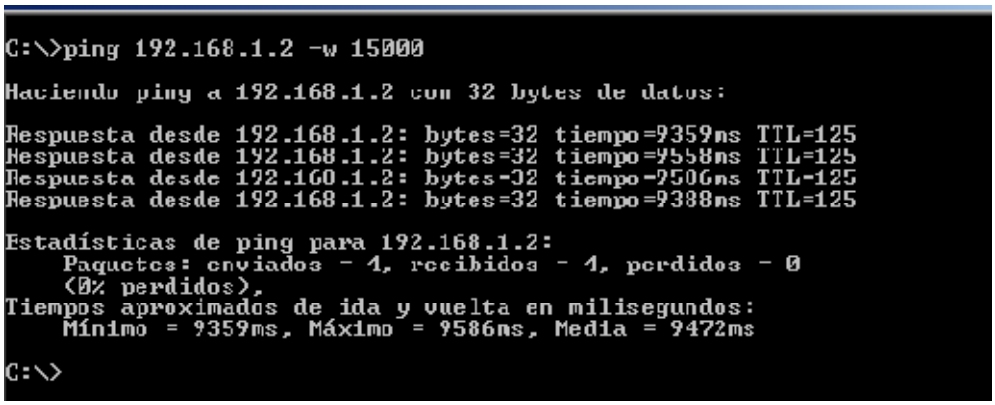


Figura 4.20 – Resultado de Ping desde PC3 al PC4

Fuente: http://es.scribd.com/doc/75286465/VlAN

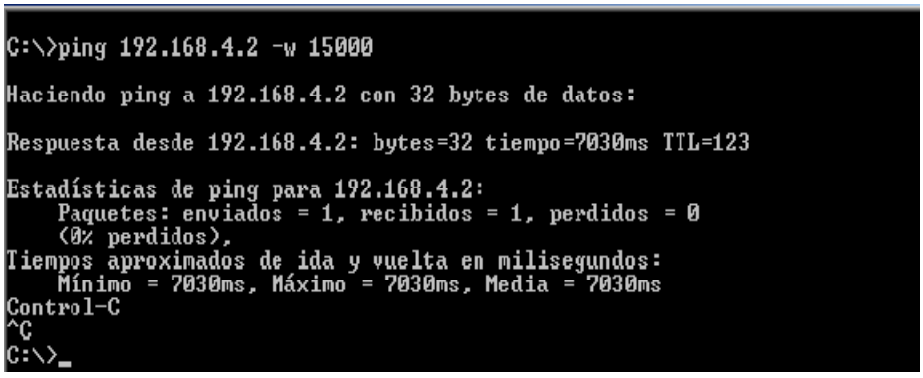


Figura 4.21 – Resultado de Ping desde PC3 al PC6

Fuente: http://es.scribd.com/doc/75286465/VlAN

Con estas dos capturas se comprueba la conectividad existente en toda la red. Detodas las capturas realizadas se aprecia algo muy significativo, esto es que los paquetes se ralentizan una vez entran en las VM, o lo que es lo mismo, cuando pasan por la redsimulada, siendo este un problema difícil de solucionar.

A continuación se mostrarán las mismas capturas, pero esta vez creada la VPN-A y laVPN-B.

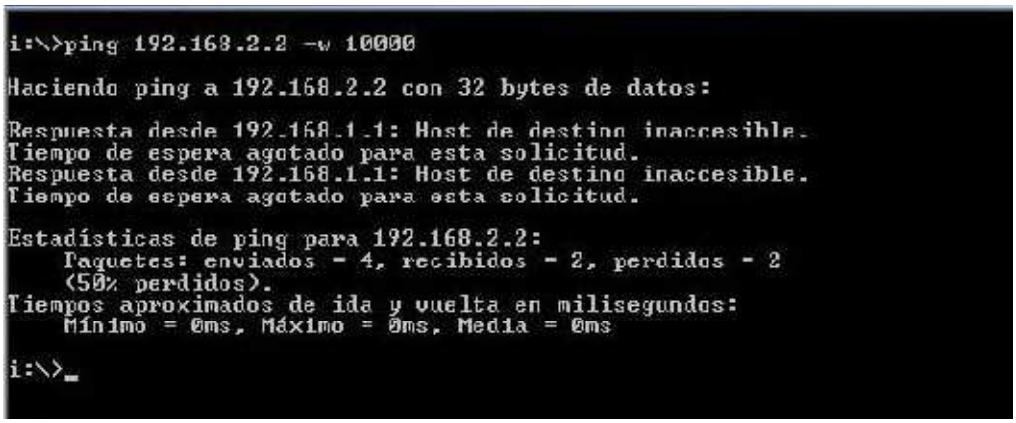


Figura 4.22 – Ping de PC4 a PC3

Fuente: http://es.scribd.com/doc/75286465/VlAN

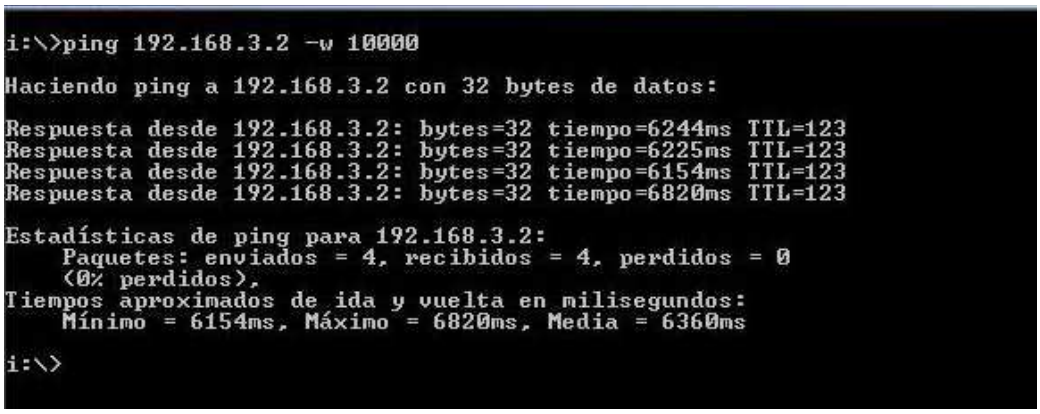


Figura 4.23 – Ping de PC4 a PC5

Fuente: http://es.scribd.com/doc/75286465/VlAN

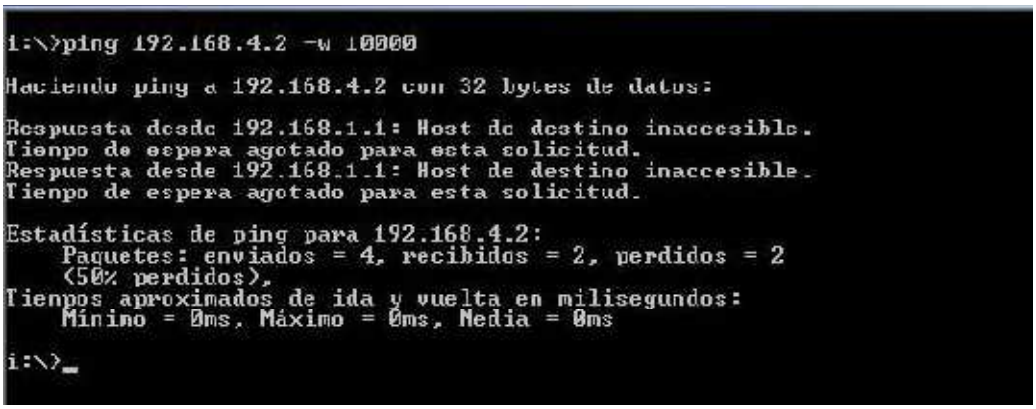
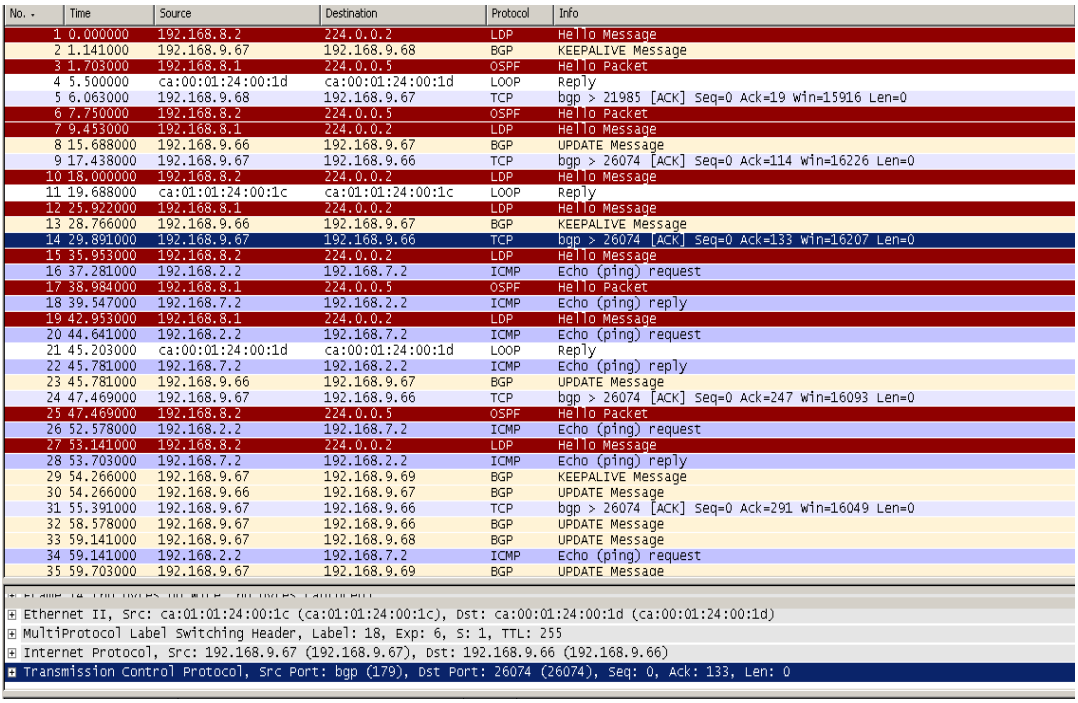


Figura 4.24 – Ping de PC4 a PC6

Fuente: http://es.scribd.com/doc/75286465/VlAN

Otras pruebas realizadas son los paquetes capturados por la red, para lo cual seutiliza elprograma *Wireshark*, además de tener que recurrir al comando ***capture***ya explicado. Pudiendo observar todo el tráfico que pasa por la interfaz.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.8.2	224.0.0.2	LDP	Hello Message
2	1.141000	192.168.9.67	192.168.9.68	BGP	KEEPALIVE Message
3	1.703000	192.168.8.1	224.0.0.5	OSPF	Hello Packet
4	5.500000	ca:00:01:24:00:1d	ca:00:01:24:00:1d	LOOP	Reply
5	6.063000	192.168.9.68	192.168.9.67	TCP	bgp > 21985 [ACK] Seq=0 Ack=19 Win=15916 Len=0
6	7.750000	192.168.8.2	224.0.0.5	OSPF	Hello Packet
7	9.453000	192.168.8.1	224.0.0.2	LDP	Hello Message
8	15.688000	192.168.9.66	192.168.9.67	BGP	UPDATE Message
9	17.438000	192.168.9.67	192.168.9.66	TCP	bgp > 26074 [ACK] Seq=0 Ack=114 Win=16226 Len=0
10	18.000000	192.168.8.2	224.0.0.2	LDP	Hello Message
11	19.688000	ca:01:01:24:00:1c	ca:01:01:24:00:1c	LOOP	Reply
12	25.922000	192.168.8.1	224.0.0.2	LDP	Hello Message
13	28.766000	192.168.9.66	192.168.9.67	BGP	KEEPALIVE Message
14	29.891000	192.168.9.67	192.168.9.66	TCP	bgp > 26074 [ACK] Seq=0 Ack=133 Win=16207 Len=0
15	35.953000	192.168.8.2	224.0.0.2	LDP	Hello Message
16	37.281000	192.168.2.2	192.168.7.2	ICMP	Echo (ping) request
17	38.984000	192.168.8.1	224.0.0.5	OSPF	Hello Packet
18	39.547000	192.168.7.2	192.168.2.2	ICMP	Echo (ping) reply
19	42.953000	192.168.8.1	224.0.0.2	LDP	Hello Message
20	44.641000	192.168.2.2	192.168.7.2	ICMP	Echo (ping) request
21	45.203000	ca:00:01:24:00:1d	ca:00:01:24:00:1d	LOOP	Reply
22	45.781000	192.168.7.2	192.168.2.2	ICMP	Echo (ping) reply
23	45.781000	192.168.9.66	192.168.9.67	BGP	UPDATE Message
24	47.469000	192.168.9.67	192.168.9.66	TCP	bgp > 26074 [ACK] Seq=0 Ack=247 Win=16093 Len=0
25	47.469000	192.168.8.2	224.0.0.5	OSPF	Hello Packet
26	52.578000	192.168.2.2	192.168.7.2	ICMP	Echo (ping) request
27	53.141000	192.168.8.2	224.0.0.2	LDP	Hello Message
28	53.703000	192.168.7.2	192.168.2.2	ICMP	Echo (ping) reply
29	54.266000	192.168.9.67	192.168.9.69	BGP	KEEPALIVE Message
30	54.266000	192.168.9.66	192.168.9.67	BGP	UPDATE Message
31	55.391000	192.168.9.67	192.168.9.66	TCP	bgp > 26074 [ACK] Seq=0 Ack=291 Win=16049 Len=0
32	58.578000	192.168.9.67	192.168.9.66	BGP	UPDATE Message
33	59.141000	192.168.9.67	192.168.9.68	BGP	UPDATE Message
34	59.141000	192.168.2.2	192.168.7.2	ICMP	Echo (ping) request
35	59.703000	192.168.9.67	192.168.9.69	BGP	UPDATE Message

Figura 4.25 – Captura de la interfaz f1/0 entre PE1 y P (VM2)

Fuente: http://es.scribd.com/doc/75286465/VlAN

4.3.7. Escenario 7: Simulación de Acceso remoto

Una vez realizadas todas las pruebas oportunas sobre el funcionamiento de la herramienta Dynagen/Dynamips y de su interfaz gráfica *GNS3*, se está en disposición de crear un escenario externo con el cual se pueda conectar un ordenador que no pertenezca a la red anteriormente diseñada (ver figura 4.15).

Para este ensayo, lo primero que se pretende realizar es una simulación de las distintas redes que debería de atravesar un ordenador para alcanzar uno de los **routers** Cisco frontera diseñados en el apartado anterior (Figura 4.15). Se simplificará el escenario dejando únicamente una VM y una red, aunque realmente esté conectado a toda la red como se realizó en el apartado anterior.(Martin, 2008)

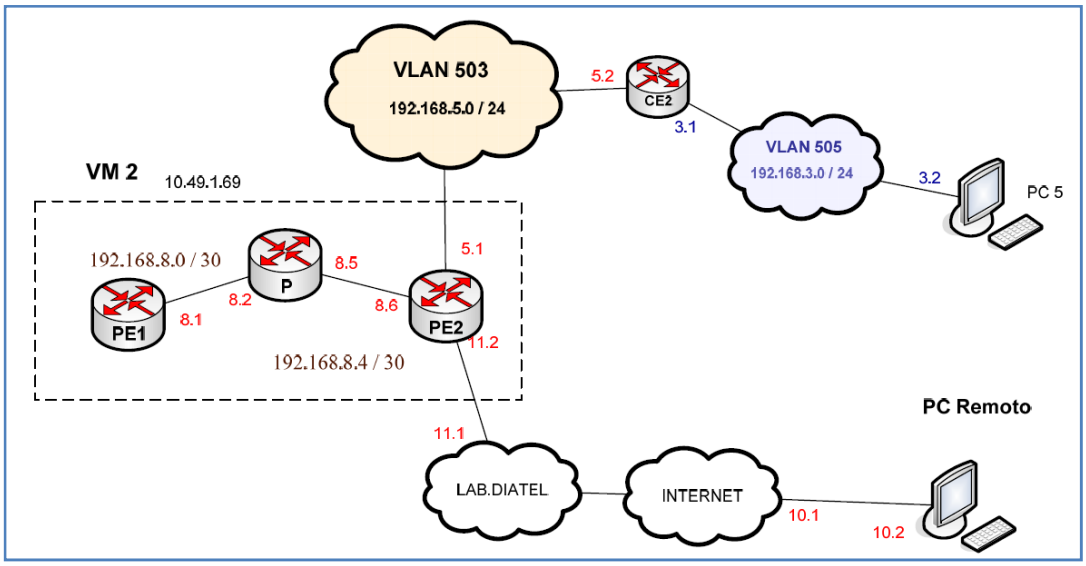


Figura 4.26 – Escenario de conexión remota

Fuente: http://es.scribd.com/doc/75286465/VlAN

Para la simulación del acceso remoto los pasos que se siguen son los siguientes:

Primero el ordenador remoto es un PC cualquiera, después para simular tanto las red de internet como de Laboratorio lo que se hace es crear una red con *routers*reales.

La única diferencia que hay entre internet y una red creada localmente, es que en la red local sólo pasará por un número reducido de *routers*, mientras que por internet pasara por un número indeterminado de *routers*.

En cambio para la simulación de la red de *LAB DIATEL*se simplificará, ya que en la realidad existirían unos firewall que se deberían autorizar a pasar, mientras que en la red simulada sólo se tendrá que pasar por unos *routers*.

Como se ha realizado hasta el momento con un ping se podría comprobar que entre ambas redes existe conectividad. En este escenario no tendría sentido realizar untracerouter, ya que si se pretende simular internet debería pasar por un númeroindeterminado de *routers*.

Después de detallar como quedaría configurada la red, se puede asegurar que unusuario que acceda desde un ordenador remoto tendrá conectividad, no sólo concualquiera de las PC sino que también con todos los *routers*. Para ello hay queconfigurar el enlace entre el *LAB DIATEL*y *router*Cisco “PE2” con la VPN con la quese quiera conectar.

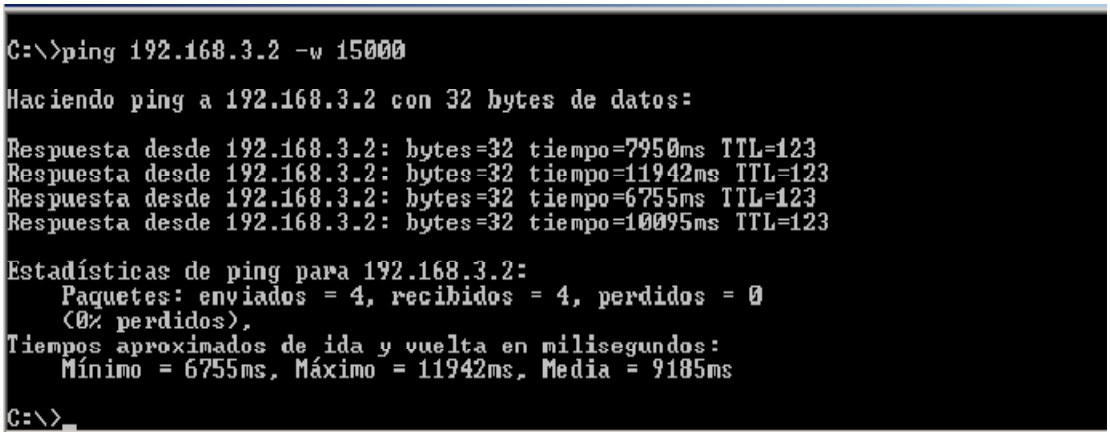


Figura 4.27 – Ping de PC remoto a PC5

Fuente: http://es.scribd.com/doc/75286465/VlAN

Se demuestra entonces que, al igual que este ordenador remoto puede acceder al escenario simulado (Figura 4.15), cualquier ordenador que quiera acceder al escenario simulado no tendría ningún problema, sólo se necesitará tener un enlace entre el ordenador y el *router*Cisco deseado.

4.3.8. Escenario 8: Creación VLAN de Gestión

Este será el último escenario que se creará con la aplicación *GNS3*, por lo que se unirán todos los escenarios hasta ahora desarrollados. Al mismo tiempo se introducirá un elemento esencial con el que se podrá implantar el laboratorio virtual, lo que será indispensable introducir en el escenario será una VLAN de Gestión, con la que se pueda acceder a todos los *routers*Cisco Simulados de la red. Para ello se requiere que la VLAN de Gestión tenga un enlace directo con cada *router*con el que se quiera tomar el control.
Debido a que el escenario consta de dos VM, para realizar estos ensayos se conectará la VLAN de Gestión con una única VM, ya que una vez comprobado que puede conectar con una *VM*, queda demostrado que puede trabajar con tantas como se desee, sólo se requerirá de un procesador lo suficientemente potente que lo soporte.

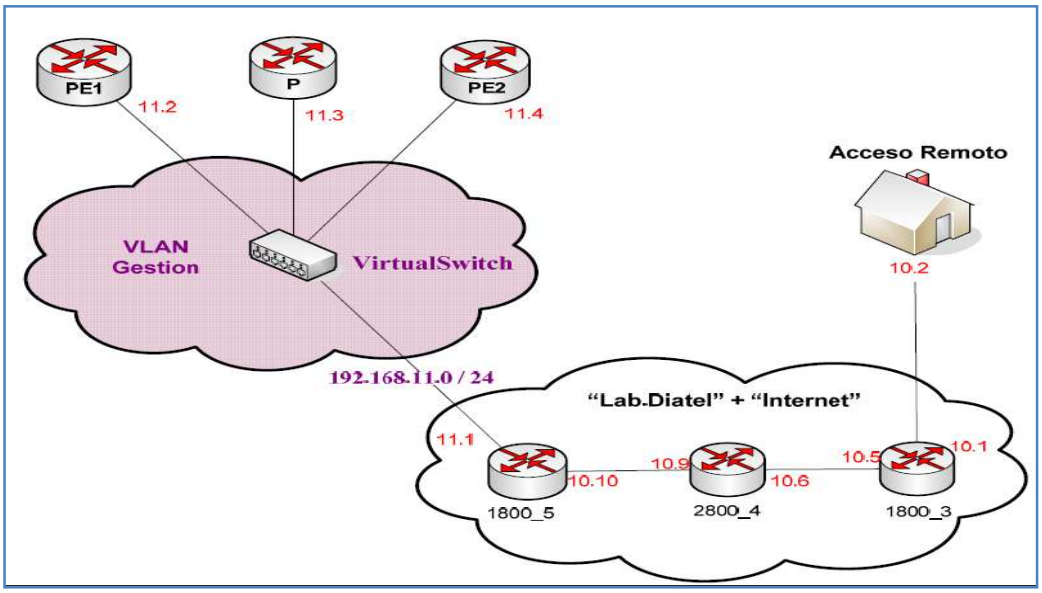


Figura 4.28 – Creación de VLAN de Gestión

Fuente: http://es.scribd.com/doc/75286465/VlAN

Como se puede observar en la Figura 4.28 la creación de la VLAN de Gestión se hará mediante un switch. La VLAN de gestión tiene acceso a cualquiera de los *routers*Cisco. En la Figura 4.28 además se detalla la manera en la que se simula la creación de las redes de Internet y *LAB DIATEL*.

Un punto esencial para la creación de la VLAN de Gestión se va a poder visualizar en la siguiente figura, en la que se detallará como se crea con la herramienta de *GNS3*.

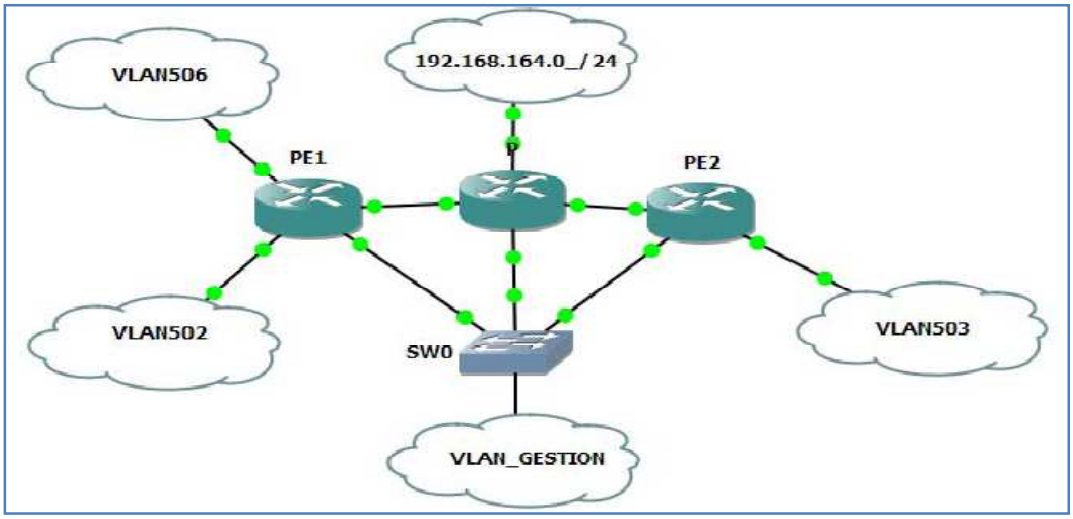


Figura 4.29 – Escenario VLAN de gestión en GNS3

Fuente: los autores (Simulador GNS3)

En este caso bastará con crear una única VLAN para todos los *routers*, por lo que con un único *switch*se creará la VLAN de Gestión. Pero en el caso de necesitar diferentes VLAN se tendrá que seguir la misma filosofía utilizada en las interfaces etiquetadas, en la Figura 4.31 se realizará un ejemplo. Para poder crear un único puerto compartido entre varias VLAN se tendrá que realizar con diferentes redes en *GNS3*, aunque físicamente se esté trabajando con una única tarjeta de red Ethernet tal y como ocurría en la creación de las interfaces etiquetadas.

Como se puede comprobar, gracias a la VLAN de Gestión un usuario se va a poder conectar con cualquier *router*. Hay que tener claro que la VLAN de Gestión será transparente para los usuarios.

A continuación se mostrará el escenario completo, integrando todos los escenarios creados en este apartado. Se podrá observar que no está el *Web Server*, esto es debido a que para no enrevesar demasiado el escenario, se ha prescindido del *Web Server*, aunque su configuración no tenga mayor complejidad.

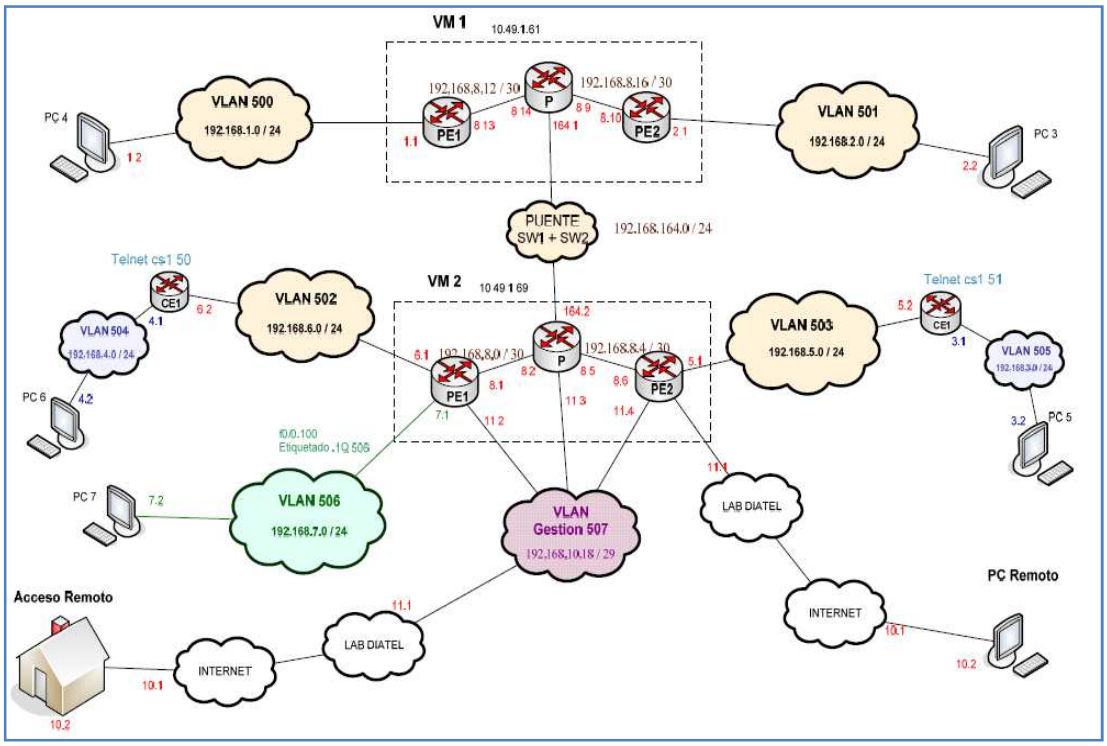


Figura 4.30 – Escenario completo VLAN de gestión

Fuente: http://es.scribd.com/doc/75286465/VlAN

Como se puede comprobar tanto el acceso remoto como el PC remoto tienen las mismas direcciones, eso es debido a que se están simulando dos conexiones independientes de un mismo ordenador, una conexión para tomar el control de los *routers*y otra para poder pertenecer a la misma red.

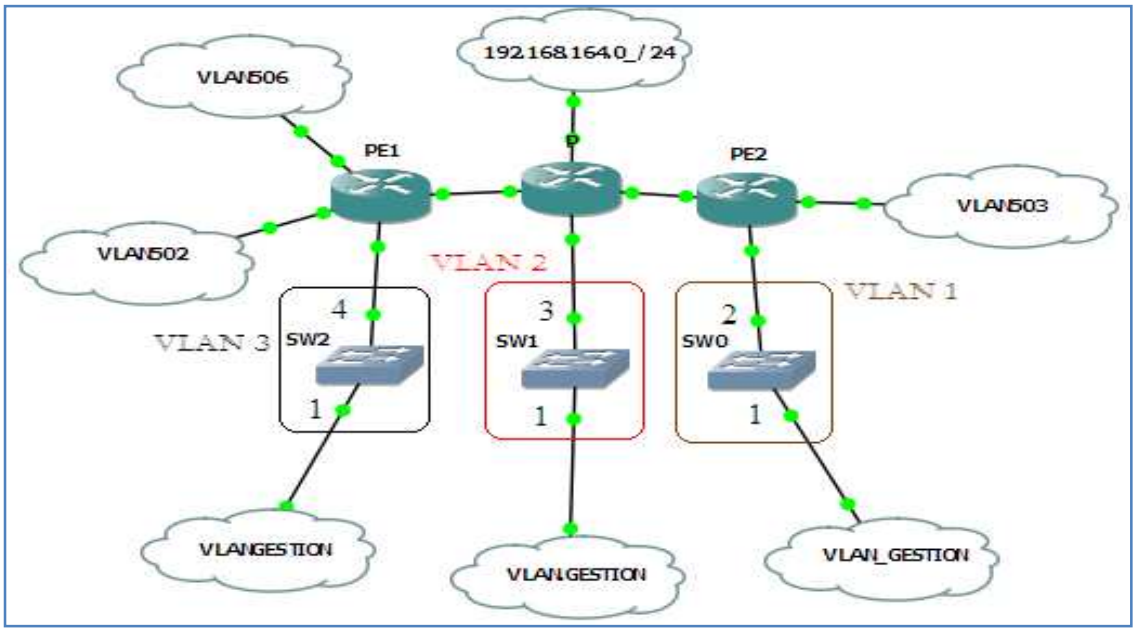


Figura 4.31 – Creación de VLAN con GNS3

Fuente: los autores (Simulador GNS3)

Después de realizar la simulación de cómo se comparten los puertos de un switchpara crear diferentes VLAN, se realizarán las pruebas oportunas para comprobar sufuncionamiento. Pero antes de poder realizar ninguna prueba, primero se configuraránlos *routers*para permitir que diferentes usuarios puedan acceder a ellos. Esto seconseguirá accediendo a cada uno de los *routers*y asignándole una contraseña, ademásde configurarle en modo virtual donde se le tendrá que indicar cuantos usuarios puedenacceder a la vez (ver Anexo V). También **se necesitará instalar un servidor de conexiones Telnet (por ejemplo: *freeSSHD*)** en la VM donde se encuentra creada laVLAN de Gestión. En el PC remoto se utilizará cualquier herramienta que proporcioneconsolas, las cuales se utilizarán para realizar conexiones con los diferentes *routers*. Por tanto una vez esteconfigurado se mostrarán los resultados obtenidos comprobando el comportamiento dela VLAN de Gestión.

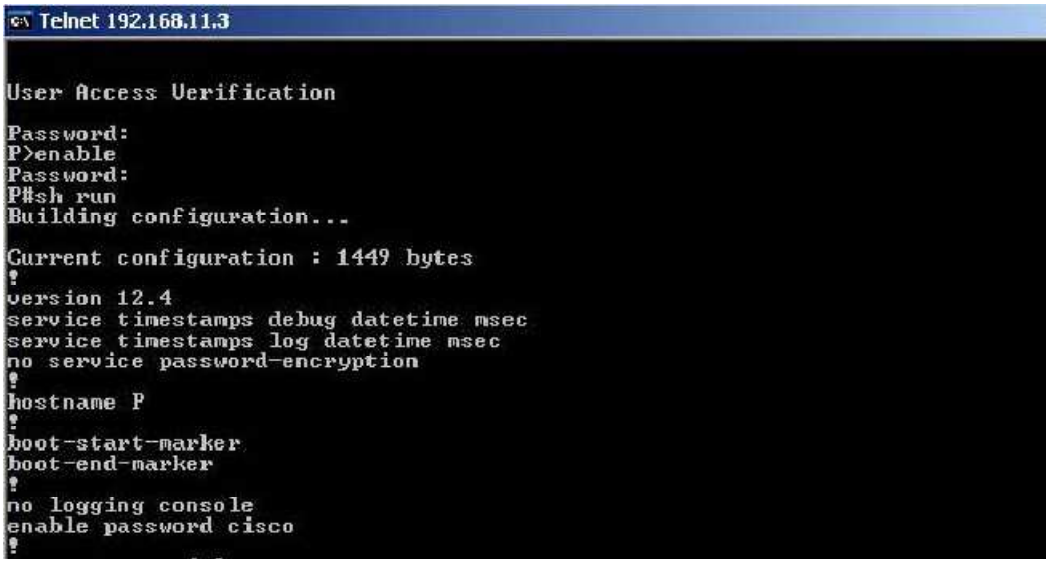


Figura 4.32 – Conexión remota al router P

Fuente: http://es.scribd.com/doc/75286465/VlAN

Como se puede observar en la Figura 4.32 se ha realizado un *telnet* desde el PCremoto al *router*Cisco "P" tomando su control, pudiendo modificarlo tanto en laconsola remota como desde el propio *router*. A continuación se mostrarán los resultadosobtenidos de los otros dos *routers*.

Figura 4.33 – Conexión remota al router PE1

Fuente: http://es.scribd.com/doc/75286465/VlAN

Figura 4.34 – Conexión remota al router PE2

Fuente: http://es.scribd.com/doc/75286465/VlAN

Como se puede comprobar en todos los casos se pide una contraseña como se ya ha mencionado, ésta sólo permitirá el acceso a los usuarios autorizados. En los ensayos realizados se demuestra como desde un lugar remoto se ha podido acceder a los *routers* Cisco simulados siendo esto el principio del laboratorio de Telemática, asimismo éste es el principal objetivo del proyecto, aunque no el único ya que hay muchas variantes dentro del mismo lado del networking como las migraciones de tecnologías, etc.

CAPÍTULO 5

PRESUPUESTO APROXIMADO DEL COSTO PARA INTEGRACIÓN DE LA MATERIA LABORATORIO DE TELEMÁTICA

A continuación mostraremos un análisis de los costes que nos conllevaría para la realización de este laboratorio. Especificando los costes de: equipos hardware, programas software y los recursos humanos requeridos. También se añadirán los componentes necesarios para la realización de la documentación.

Dentro del costo de software se ha considerado obtener Microsoft Windows 7 con su respectiva licencia, esto debido a que los ensayos estudiados anteriormente se lo realizo con GNS3 Standalone 64 bits que es la última versión actualizada y solo es compatible con Windows 7 64 bits y en este ya incluye todos sus complementos como Dynagen, Putty, entre otras. En este caso no se compraría Windows 8 debido a que no existe un GNS3 para trabajar sobre dicha plataforma.

Tabla 5.1 Costes del software

PROGRAMAS	CANTIDAD	PRECIO	PRECIO TOTAL
VMware Server	1	$0.00	$ 0.00
Microsoft Windows 7	2	$ 170.00	$ 340.00
Microsoft Office	1	$ 140.00	$ 140.00
Microsoft Visio Professional	1	$ 60.00	$ 60.00 $
Dynamips	1	$ 0.00	$ 0.00
IOS Cisco	1	$ 500.00	$ 500.00
GNS3	1	$ 0.00	$ 0.00
Wireshark	1	$ 0.00	$ 0.00
freeSSHD	1	$ 0.00	$ 0.00
		TOTAL:	**$ 1,040.00**

Fuente: los autores

Tabla 5.2 Costes de equipos físicos

EQUIPOS FISICOS	CANTIDAD	PRECIO	PRECIO TOTAL
Servidor ACER AAG540	1	$ 1100.00	$ 1,100.00
PC’s para laboratorio	8	$ 600.00	$ 4,800.00
Router Cisco	3	$ 400.00	$ 1,200.00
Switch Configurable Cisco	1	$ 550.00	$ 550.00
Router Atlas 350	2	$ 350.00	$ 350.00
Portátil HP	1	$ 1,000.00	$ 1,000.00
		TOTAL:	**$ 9,000.00**

Fuente: los autores

Tabla 4.3 Costetotal del proyecto

	PRECIO TOTAL
Coste equipos físicos	$ 9,000.00
Coste de Software	$ 1,040.00
Coste Total	**$10,040.00 $**

Fuente: los autores

Cabe indicar que dentro de estos precios aproximados se está incluyendo el IVA, además si el proyecto fuera orientado hacia otra Universidad se debería cobrar también las horas que se trabajara durante este proyecto es decir, horas de Ing. Jr. y director de proyecto, pero como en este caso es un proyecto para el desarrollo de la Facultad Técnica los recursos a usar para la implementación del proyecto serán los mismos estudiantes, que estén en busca de una tesis para obtención del título de Ingeniero en Telecomunicaciones, esto para evitar costos de mano de obra y en lo respecta a software y hardware esto deberá ser financiado por la Facultad Técnica para el desarrollo debido a que es un laboratorio nuevo para nuestra facultad.

Además los costes mencionados referentes tanto a aplicaciones software como hardware se podrán utilizar en la realización de otros proyectos, por lo que se consideran costes reutilizables, de este modo una cuantía de estos equipos repercutirá en los costes de otros proyectos.

CAPÍTULO 6
CONCLUSIONES Y FUTUROS TRABAJOS

1.1 Conclusiones

- Con todo lo desarrollado en estos escenarios para la integración de la materia Laboratorio de Telemática podemos asegurar que se han cumplido todos los propósitos que se ha planteado en un principio.

  Contando con las mismas ventajas con las que cuenta un *router*real, permitiendo el acceso múltiple a los diferentes *routers*y pudiendo protegerlos para que ninguna persona no autorizada pueda acceder a ellos.
- Las sensaciones sobre esta aplicación resultan muy esperanzadoras de cara a la implementación de este laboratorio virtual, una vez que se ha comprobado que la toma de control de las consolas sepuede realizar de forma segura, además de realizar escenarios lo suficientementecomplejos.
- En este proyecto se han ido creando escenarios de complejidad creciente, lo que nos permitió conocer las características y limitaciones de cada aplicación explorada. La resolución de los escenarios ha permitido aprender de ellos pudiendo abordar otros nuevos más ambiciosos, teniendo siempre en mente cual era el objetivo a lograr.
- Para este proyecto se ha decidido que la mejor herramienta para la realización de los laboratorios virtuales es Dynamips. Además se ha experimentado con otras aplicaciones, como el WireShark para las capturas de los paquetes y así poder observar un comportamiento más a fondo de cómo actúa una Red Privada Virtual usando protocolos a nivel de capa 2 y 3 como MPLS.
- No cabe duda que esta investigación será altamente escalable, flexible y transportable para la realización de otros proyectos o a la integración de nuevos proyectos que ya tengan que ver ya sea con la realización de prácticas más avanzadas en lo que respecta al networking ya que el mundo de las tecnologías en redes es sumamente amplio y está en constante crecimiento o en la creación de nuevos laboratorios de otras cátedras para la Facultad Técnica.

1.2 Futuros Trabajos

- Este proyecto será una buena base para aquellos estudiantes que desean completar el objetivo de la creación de un laboratorio de Telemática para la Facultad técnica ya que aquí se encontrara la base del estudio y la metodología para llevar a cabo este proceso, los estudiantes deberán analizar detenidamente cada uno de los escenarios creados en este proyecto y a partir de aquello crear prácticas para el nuevo laboratorio con sus respectivas guías de estudio, manuales y configuraciones.

- Esta experimentación ha dejado el camino abierto para la realización de nuevos proyectos, con los que se podrá concluir la creación de laboratorios virtuales. Para llegar a este fin habrá que seguir ensayando con los escenarios ya creados, es decir se podrán crear escenarios mucho más complejos para que el estudiante salga con mayor conocimiento en el área del networking.

- En los futuros escenarios se necesitará comprobar la posibilidad de poder repartir la carga de trabajo, para que no sea un mismo ordenador el que lo soporte.
  También se deberán buscar alternativas para que diferentes usuarios accedan a las máquinas virtuales correspondientes pudiendo utilizar los **routers**creados en dicho escenario.

- Igualmente, será necesario realizar pruebas desde escenarios reales, teniendo que poder soportar no sólo todas las posibles conexiones, sino que también deberá acceder por redes inseguras como puede ser Internet o acceder a través de *firewall* para poder llegar al servidor correspondiente.

REFERENCIAS Y BIBLIOGRAFÍAS

Anuzelli, G. (s.f.). *GNS3 Documentación.* Recuperado el 2012, de iloo files wordpress: http://iloo.files.wordpress.com/2009/07/gns3-0-4-1_documentation_spanish.pdf

CISCO 1, Networking Academy. (26 de Octubre de 2010). *CCNA 1 Exploration: Aspectos Basicos de Networking.* Recuperado el 22 de Octubre de 2012, de http://www.slideshare.net/liberaunlibroupeg/ciscoccna1explorationaspectosbasicosdenetworkingversion40espanol

CISCO 2, Networking Academy. (17 de febrero de 2009). *CCNA 2 Exploration: Concepto y Protocolos de Enrutamiento.* Recuperado el 22 de octubre de 2012, de http://es.scribd.com/doc/12487509/Cisco-CCNA-2-Exploration

David Luna, V. C. (15 de marzo de 2005). *Switching a nivel 3.* Recuperado el 23 de octubre de 2012, de http://locortes.net/Vicenc/Telematica/Enginyeria%20de%20Xarxes/

Edson Alexander Hernández Gámez, J. A. (marzo de 2012). *Biblioteca virtual Universidad Tecnologica de El Salvador.* Recuperado el abril de 2013, de Implementación de un prototipo de telefonía IP a nivel de software, que facilite la comunicación entre los usuarios en la Facultad de Informática y Ciencias Aplicadas: http://biblioteca.utec.edu.sv/siab/virtual/tesis/55320.pdf

GALLEGOS, E. D. (28 de junio de 2012). *Repositorio de Datos ESPOCH.* Recuperado el febrero de 2013, de http://dspace.espoch.edu.ec/handle/123456789/1933?mode=full

Ghein, L. D. (2007). *MPLS Fundamentals.* Indianapolis USA: Cisco Press.

GNS3 Graphical Network Simulator. (2007). *GNS3 Documentación*. Recuperado el 2012, de http://www.gns3.net/documentation/

Mario. (8 de mayo de 2013). *Geeky Theory*. Recuperado el mayo de 2013, de Tutorial Wireshark: http://www.geekytheory.com/tutorial-wirshark-1-instalacion/

Martin, R. H. (27 de noviembre de 2008). *Scribd.* Recuperado el 29 de octubre de 2012, de http://es.scribd.com/doc/75286465/VlAN

Martínez, I. M. (2009). *MODELO PARA EL DESARROLLO DE SERVICIOS ATM Y FRAME RELAY*. Recuperado el FEBRERO de 2013, de http://www.oocities.org/es/marbry69/e3/T_2.htm

Networkeando. (29 de noviembre de 2008). Recuperado el febrero de 2013, de Frame Relay en GNS3: http://networkeando.blogspot.com/2008/11/frame-relay-en-gns3.html

Orihuela, P. S. (s.f.). *Repositorio Universidad Carlos III de Madrid.* Recuperado el febrero de 2013, de DISEÑO DE UNA RED VPLS JERÁRQUICA: http://e-archivo.uc3m.es/bitstream/10016/11909/1/PFC%20VPLS-Pablo%20Sesmero.pdf

PUPIALES, S. K. (2012). *Repositorio Universidad Tecnica del Norte - Ibarra.* Recuperado el febrero de 2013, de http://repositorio.utn.edu.ec/bitstream/123456789/751/1/04%20RED%20001%20BACKBONE%20MPLS%20Y%203PLAY.pdf

Segundo, J. d. (2009). *Introducción a los servicios de red e Internet*. Recuperado el octubre de 2012, de http://jorgedenovasri.files.wordpress.com/2012/09/gns3.pdf

Teillier, F. (s.f.). *Lectura Frame Relay.*Recuperado el febrero de 2013, de ganimides: http://ganimides.ucm.cl/partime/fteillier/f-relay.pdf

ANEXOS

ANEXO I – Configuración OSPF y MPLS

Configuración de interfaces OSPF:

router>enable
router # configure terminal
router(config)# hostname PE1
router(config)# router ospf<identificador del proceso OSPF >

PE1(config)# router ospf 1
router(config)# network <dirección IP>< wildcard-mask> area <area-id>
PE1(config)# network 192.168.1.0 0.0.0.255 area 0

Configuración de interfaces MPLS-LDP
router>enable
router # configure terminal
router (config)# hostname PE1

Para activar CEF y poder trabajar en entornos MPLS:
PE1(config)# ipcef

Para activar el protocolo de distribución de etiquetas LDP:
router (config)# interface fastethernet<nombre de la interfaz>
PE1(config)# interface fastethernet1/0
PE1(config-if)# mplsip
PE1(config-if)# mpls label protocol ldp

ANEXO II – Configuración de interfaces

router>enable

router # configure terminal

Cambiar el nombre:

router(config)# hostname <nombre>

router(config)# hostname PE2

Desactivar los log de Cisco

PE2(config)# no loggingconsole

router(config)# interface fastethernet<nombre de la interfaz>

PE2(config)# interface fastethernet f1/0

router (config-if)# ip address <dirección IP><máscara>

PE2(config-if)# ip address 192.168.164.4 255.255.255.224

Para activar la interfaz:

PE2(config-if)# no shutdown

ANEXO III – Configuración interfaz etiquetada 802.1Q

router>enable

router # configure terminal

router(config)# hostname PE2

PE2(config)# no loggingconsole

router(config)# interface fastethernet<nombre de la interfaz>.<número de subinterfaz>

PE2(config)# interface fastethernet f0/0.100

router(config-subif)# encapsulation dot1Q <VLAN ID>

PE2(config-subif)# encapsulation dot1Q 506

router(config-subif)# ip address <dirección IP><máscara>

PE2(config-subif)# ip address 192.168.7.1 255.255.255.224

PE2(config-subif)# exit

router(config)# interface fastethernet<nombre de la interfaz>

PE2(config)# interface fastethernet f0/0

Para activar la interfaz:

PE2(config-if)# no shutdown

ANEXO IV – Configuración VPN

Configuración de BGP

router>enable
router # configure terminal
router(config)# hostname PE2
PE2(config)# no loggingconsole
router(config)# interface <número de la interfaz>
PE2(config)# interface loopback255
router(config-if)# router bgp<número de proceso BGP>
PE2(config-if)# router bgp 65001
router(config-router)# neighbor<dirIP de la interfaz vecina enfrentada>remoteas<número de proceso BGP>
PE2(config-router)# neighbor 192.168.9.67 remote-as 65001
router(config-router)# neighbor<dir IP de la interfaz vecina enfrentada>updatesourceloopback<número de la interfaz>
PE2(config-router)# neighbor update-source loopback 255

Configuración VPN
PE2 # configure terminal
router(config) # ipvrf<nombre de la VPN>
PE2(config)# ipvrf VPN-A
router(config-vrf)# rd<valor del rd>
PE2(config-vrf)# rd 65001:41
router(config-vrf)# router-target export <valor quetienequeexportar>
PE2(config-vrf)# router-target export 65001:400
router(config-vrf)# router-target import<valor que tiene que importar>
PE2(config-vrf)# router-target import 65001:400

Se podrá utilizar un único comando para exportar e importar:

router(config-vrf)# router-target both<valor que tiene que exportar e importar>

PE2(config-vrf)# router-target both 65001:400

router(config)# interface <nombre de la interfaz>

PE2(config)# interface fastethernet1/0

router(config-if)# ipvrf forwarding <nombre de la VRF>

PE2(config-if)# ipvrf forwarding VPN-A

Después de este comando se volverá a pedir:

router(config-if)# ip address <dirección IP><máscara>

PE2(config-if)# ip address 192.168.8.6 255.255.255.252

ANEXO V. MANUAL GNS3

Partes de este tutorial fueron tomados del excelente tutorial de Dynagen de Greg Anuzelli.

INTRODUCCIÓN

GNS3 es un simulador gráfico de redes que permite diseñar fácilmente topologías de red y luego ejecutarlas. Hasta este momento GNS3 soporta el IOS de routers, ATM/FrameRelayswitches Ethernet y PIX firewalls. Para realizar esta magia, GNS3 está basado en:

- ***Dynamips:***Es un emulador de routers Cisco para las plataformas 1700, 2600, 3600, 3700 y 7200 ejecutándo imágenes de IOS estándar. También provee un switch virtual simple, no emula switchesCatalyst (aunque si emula la NM-16ESW).
- ***Dynagen:***Es un frontend basado en texto para Dynamips elaborado por Greg Anuzelli para interactuar con Dynamips. GNS3 también utiliza el formato .INI de configuración e integra la consola de administración de Dynagen que permite a los usuarios listar los dispositivos, suspender y recargar instancias, determinar los valores de Idle-PC, realizar capturas, entre otros.
- ***Pemu:***Un servidor de seguridad PIX de Cisco, para salvar las configuraciones.

IMÁGENES IOS

En Windows, la imagen se debe ubicar en C:\Program Files\Dynamips\images o en cualquier ubicación que se desee, en los laboratorios se buscará esta locación. En sistemas Linux/Unix ubicar las imágenes en los lugares designados (de preferencia /opt/images).

Las imágenes Cisco IOS están comprimidas. Estas imágenes comprimidas funcionan bien con Dynamips, aunque el proceso de arranque es significativamente más lento debido a la descompresión (igual que en los routers reales). Es recomendable descomprimir las mismas de antemano así el emulador no tiene que realizar esa tarea. En sistemas Linux/Inx/Cygwin puede utilizar el utilitario “unzip”:

Unzip –p c7200-g6ik8s-mz.124-2.T1.bin > c7200-g6ik8s-mz.124-2.T1.image

Recibe un mensaje de advertencia del unzip, pero puede ignorarlo. En Windows se puede descomprimir las imágenes utilizando el WinRAR. Hay que tener en cuenta que las imágenesactuales de los routers 1700 y 2600 deben ser descomprimidas antes de utilizarlas en Dynamips. Siempre se debe probar las imágenes directamente con Dynamips antes de usarlas con GNS3:

./Dynamips –P <chassis><path-to –the-ios-image>

UTILIZACIÓN DE LOS RECURSOS

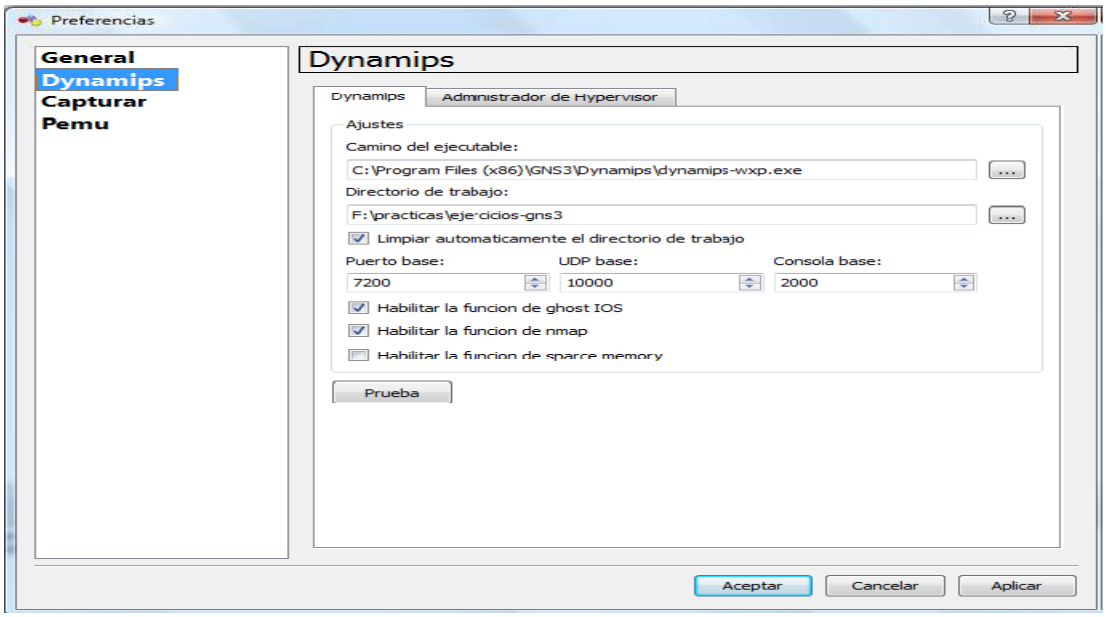
Dynamips hace uso intensivo de memoria RAM y CPU en orden de lograr la magia de la emulación. Si la intención es ejecutar una imagen de IOS que requiere 256 MB de RAM en un router 7200 real, y dedica 256 MB de RAM a la instancia de su router virtual, este utilizará 256 MB de memoria para funcionar. Dynamips también utiliza por defecto 64 MB de RAM por cada instancia en sistemas Unix y 16 MB en Windows para cachear (caché) las transacciones JIT. Este será el tamaño total de trabajo; esto se debe a que Dynamips debe trazar un mapa de la memoria virtual de los routers.

En el Directorio de Trabajo se encuentran los archivos temporales “ram” cuyo tamaño es igual a la memoria RAM de los routers virtuales. El Sistema Operativo cacheará en la RAM las secciones de los archivos nmap que están siendo utilizados. (Ver la sección Optimización del Uso de Memoria) las opciones de configuración, estas pueden reducir en forma significativa la utilización de la memoria.

Dynamips también hace uso intensivo del CPU porque está emulando la CPU de un router instrucción-por-instrucción. En principio no tiene manera de saber cuando el router virtual está en estado ocioso (idle), por esa razón ejecuta diligentemente todas las instrucciones que constituyen las rutinas de idle del IOS, igualmente que las instrucciones que conforman el “real” funcionamiento. Pero una vez que se haya ejecutado el proceso de “Idle-PC” para una determinada imagen de IOS, la utilización del CPU decrecerá en forma drástica.

CONFIGURANDO LAS PREFERENCIAS DE DYNAMIPS

Para utilizar Dynamips en GNS3, se debe configurar el camino para alcanzarlo y el puerto base. Estos valores serán utilizados por el Hypervisor Manager y para cargar los archivos .net. Buscar la opción Preferencias del menú Editar:



Luego hacer click en Prueba y si es satisfactorio este ítem, se ha configurado de la forma correcta.

El Directorio de Trabajo es el lugar en donde Dynamips almacena todos los archivos generados, esto incluye a la NVRAM de los router virtuales, también la bootflash, los logfiles, y otros archivos de trabajo.

Opciones:

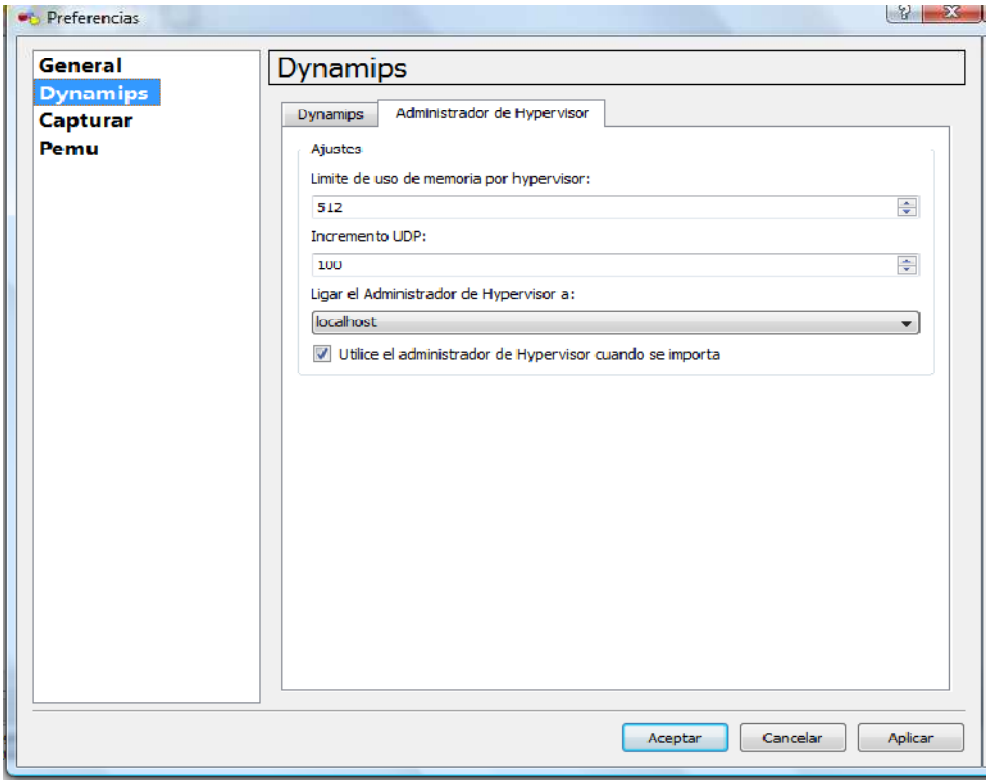
- "Habilitar la función de ghost IOS" es para utilizar la función ghost de Dynamips en forma global (o no).
- "Habilitar la función de nmap" es para utilizar la función nmap de Dynamips en forma global (o no).
- "Habilitar la función de sparcememory" es para utilizar esta función de Dynamips en forma global (o no).

Estas opciones se explican detalladamente en Optimización del uso de la memoria. El administrador Hypervisor es utilizado por GNS3 para ejecutar los hypervisors en forma interna, esto significa que no se necesita iniciarlos en forma manual. Este administrador también ayuda a resolver el problema de direccionar el límite del uso de la memoria por

cada proceso cuando varias instancias de IOS se ejecutan en un solo hypervisor, balanceando la carga de las instancias en múltiples hypervisors.

Por ejemplo se desea ejecutar 5 instancias de IOS, y cada instancia utiliza 256 MB, también se ha configurado el límite del uso de la memoria por hypervisor en 512 MB. Cuando se inicia el lab, el hypervisor creará 3 procesos de hypervisor basándose en la siguiente fórmula (el redondeo se realiza hacia el siguiente número entero):

Número de hypervisors = (256 * 5 /512)



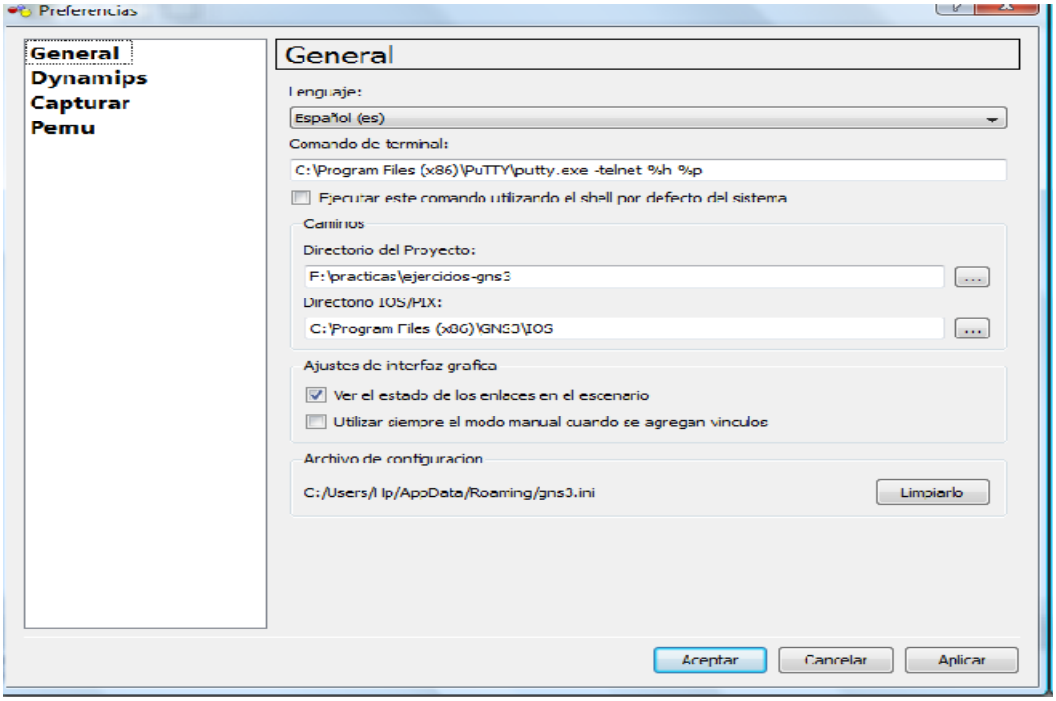
Existen dos ajustes en las Preferencias de Dynamips. “Incremento UDP” que le indica al Administrador de Hypervisor como incrementar el puerto base de Dynamips por cada proceso que el Hypervisor crea (si en las Preferencias de Dymanips el puerto base udp es de 10000 y el incremento de 100, entonces para 3 hypervisors el puerto base para el primero será de 10000, para el segundo 10100 y así sucesivamente).

La opción “Utilizar el Administrador de Hypervisor cuando se importa” se utiliza cuando se carga un archivo de topología (.net) en GNS3. Si esta opción esta marcada se ha definido que los hypervisors se ejecuten en localhost, entonces GNS3 considerara que esos hypervisors deben ser iniciados por el Administrador de Hypervisor. Si no esta

marcado, esos hypervisors deben ser iniciados como hypervisors externos y además manualmente.

CONFIGURANDO LAS PREFERENCIAS GENERALES

Para poder conectarse a las consolas de los routers virtuales, también debeconfigurar los comandos de la terminal



GNS3 le va a proponer un comando por defecto pero usted lo puede modificar.

Las siguientes son las substituciones que se realizan:

%h = host

%p = puerto

%d = nombre de dispositivo

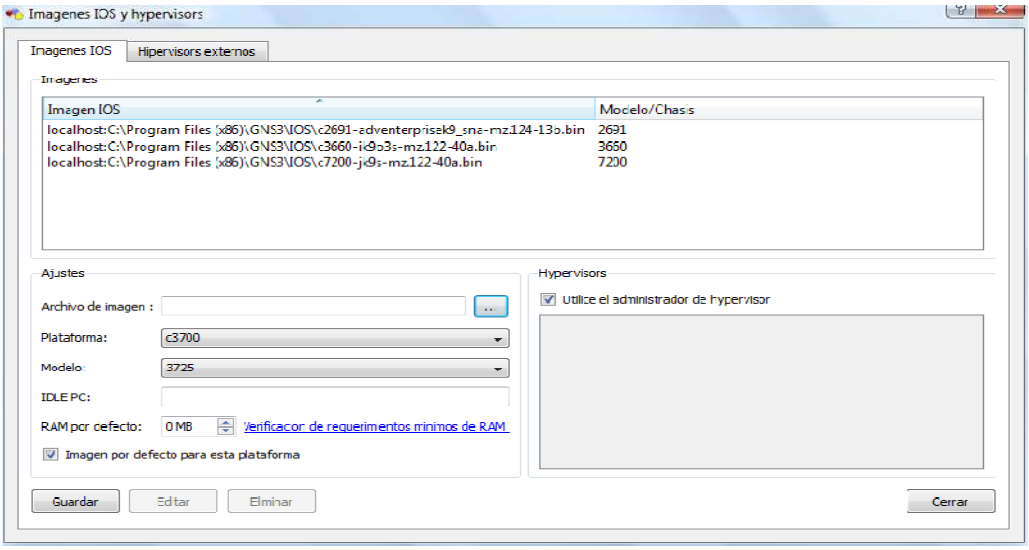
Usted tiene la opción de lanzar su comando vía un shell (cmd.exe por defecto en Windows o cualquier intérprete de comando de línea con la variable de entorno %COMSPEC% ajustada.

EJECUTANDO UN LABORATORIO SIMPLE

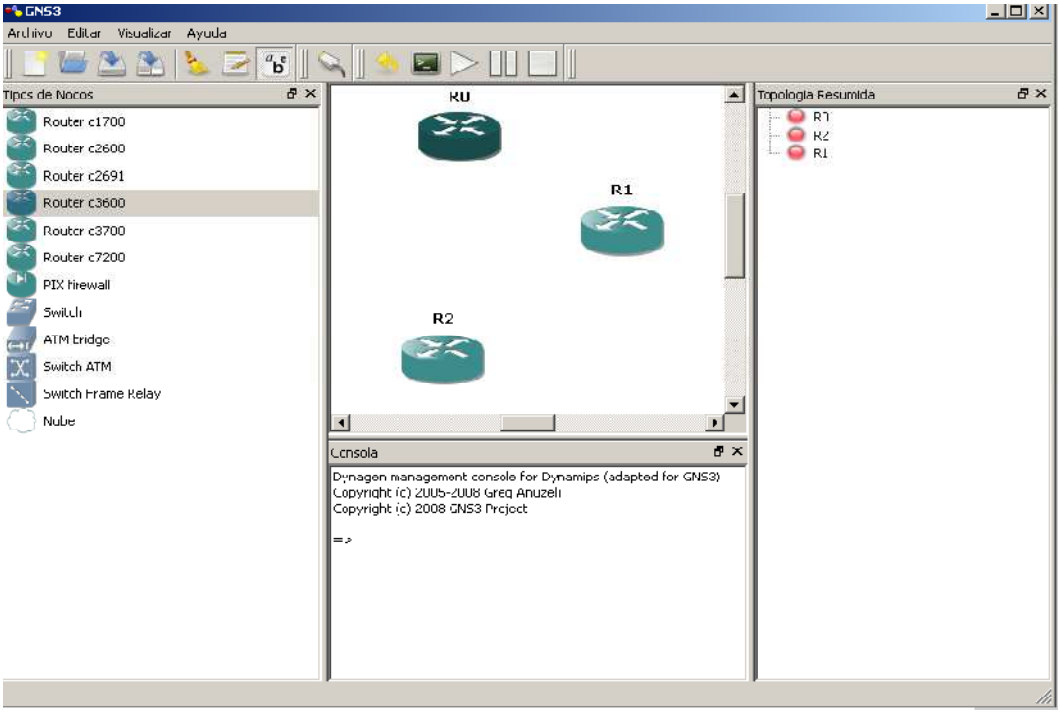
En esta sección lo guiaremos paso-a-paso para la ejecución de un lab de tresrouters.

Si inicia GNS3 por primera vez, primero debe ver la sección “Configurando las Preferencias de Dynamips”.

Primero debe registrar al menos una imagen de IOS, seleccionando Editar -> Imágenes IOS y hipervisors den menú (u oprimiendo CTRL. + MAY + I). Luegoajustar el camino al IOS, elegir la plataforma y el modelo (si es necesario) y siconoce el valor de IDLE PC ingréselo. Por defecto, se utilizara el hypervisorintegrado (GNS3 administrara los procesos Dynamips) para ejecutar los IOS.

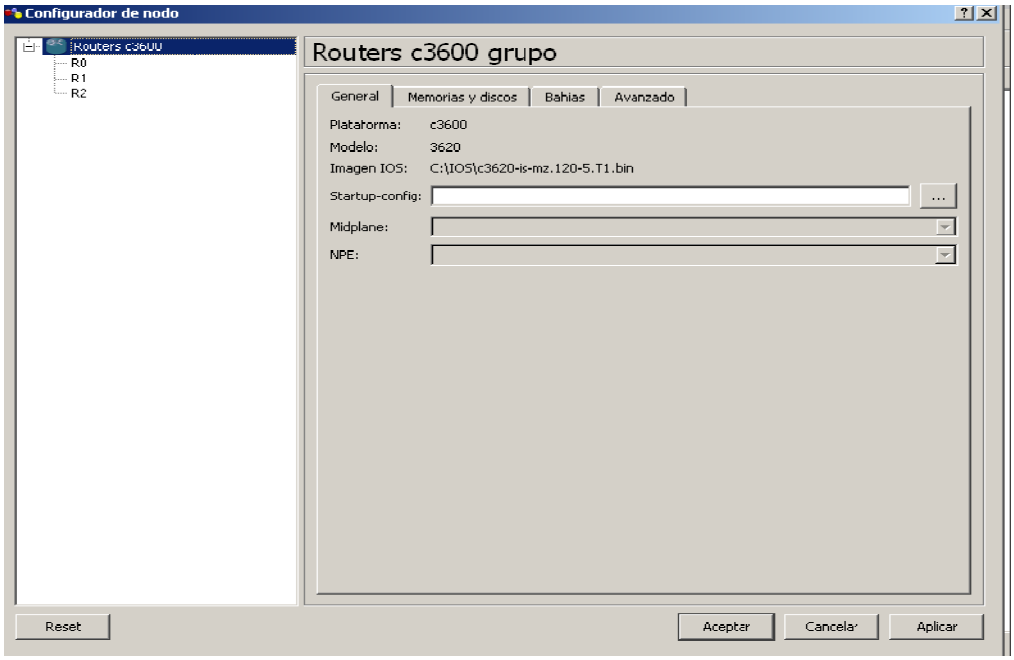


Toda la información referida a los IOS y los hypervisors será guardada en el archivo gns3.ini, por eso solo debe hacerse una vez solamente. Ahora es posible crear la topología de red solamente arrastrando los nodos que se encuentran en la lista situada a la izquierda y depositarlos en el área de trabajo.



Cuando la topología esta creada, puede proceder a configurar cada nodo (sobre el nodo indicado botón derecho del mouse y seleccionar configurar).

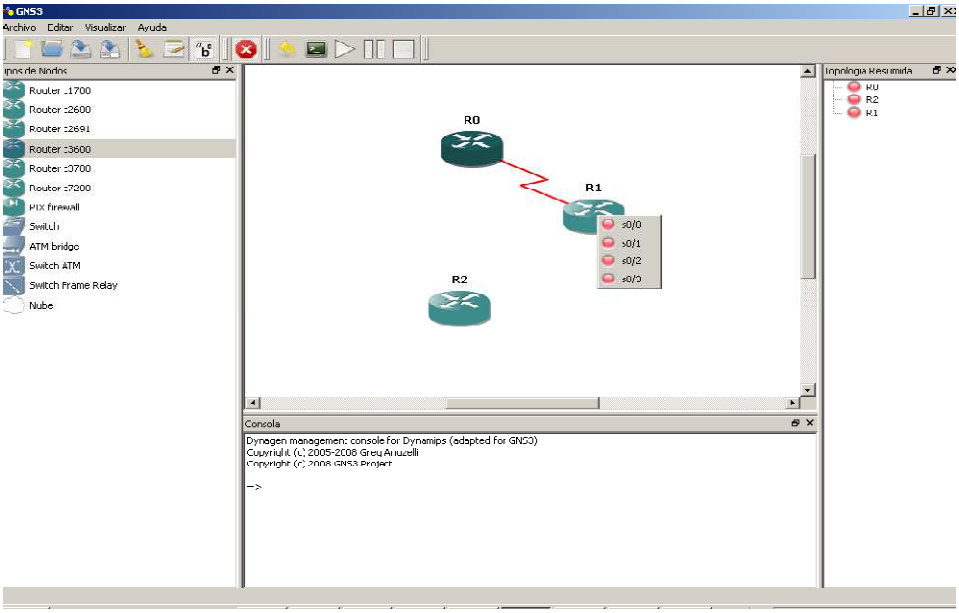
Puede aplicar la misma configuración a todos los routers seleccionando “Routers” en el árbol expandido del panel izquierdo o seleccionando un router en particular por su nombre.



En el modo de configuración de nodo usted podrá configurar varios elementos como las bahías, el tamaño de la RAM, etc.

Paso siguiente es adicionar los vínculos de cada nodo (haga clic en el botón "Agregar un vinculo" en la barra de menues y seleccione el nodo origen y destino). Notara que puede elegir el tipo de vinculo (Ethernet, serial...). GNS3 asigna automáticamente los módulos correctos correspondientes a los tipos de vínculos en las bahías de los routers y elige la primera interfaz disponible para realizar el vínculo.

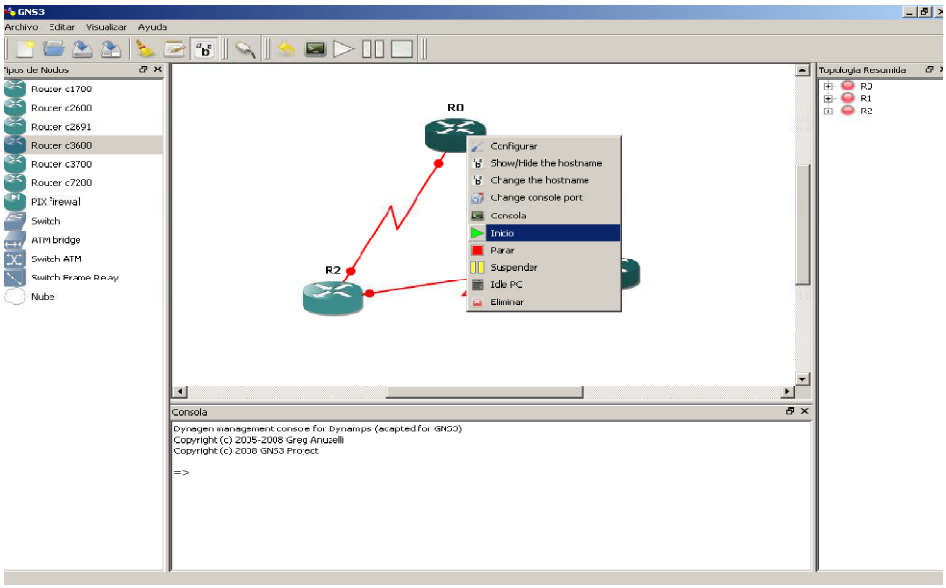
Puede seleccionar manualmente que interfaz desea conectar al vinculo, seleccionando el método manual del menú desplegable. Tenga en cuenta que tendrá que configurar las bahías de los routers en forma manual también.



Nota: Las interfaces ya utilizadas están señaladas con color verde; las disponibles en rojo.

La topología de red con todos los ajustes realizados, se crea en los hypervisors.

Usted puede iniciar/parar/suspender una instancia de IOS oprimiendo el botón derecho de mouse sobre un nodo indicado. Si ha iniciado un IOS, a continuación puede iniciar una sesión de consola en el dispositivo. Nota: múltiples nodos pueden ser seleccionados si desea realizar las operaciones simultáneamente.

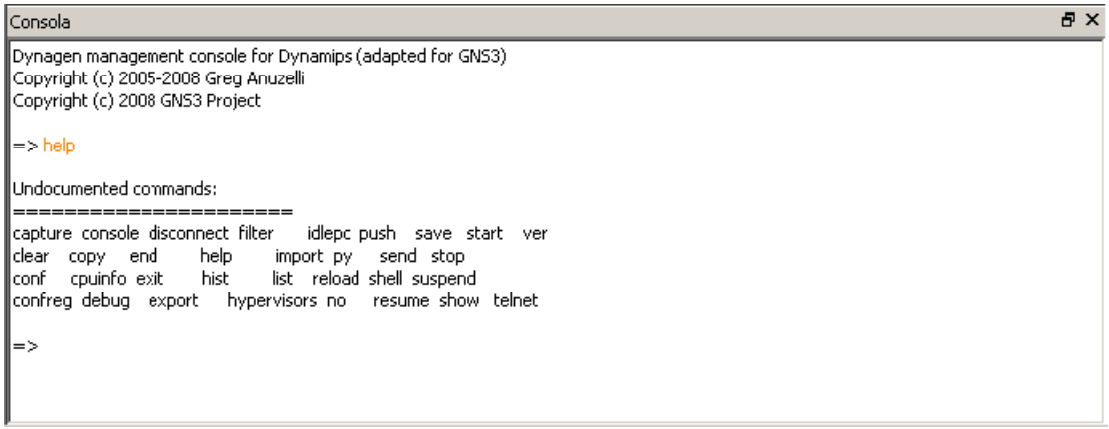


Una vez que se haya conectado a los routers vía consola, podrá asignar una dirección IP apropiada a las interfaces seriales (puede visualizar que interfaces están conectadas en el panel derecho "Topología resumida" o desplazando el mouse sobre el vinculo), y realizar el "no shut", porque están conectadas.

TRABAJANDO CON LA CONSOLA

Nota: el panel de la Consola ubicada en parte inferior estará disponible si se está a modo emulación.

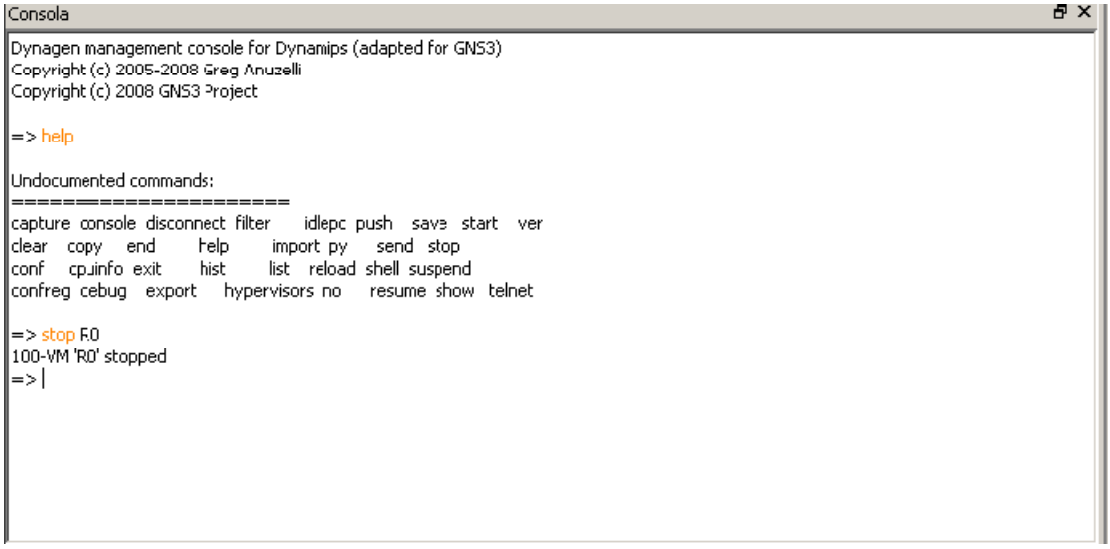
Desde la consola, utilice el comando **help**para visualizar los comandos validos:



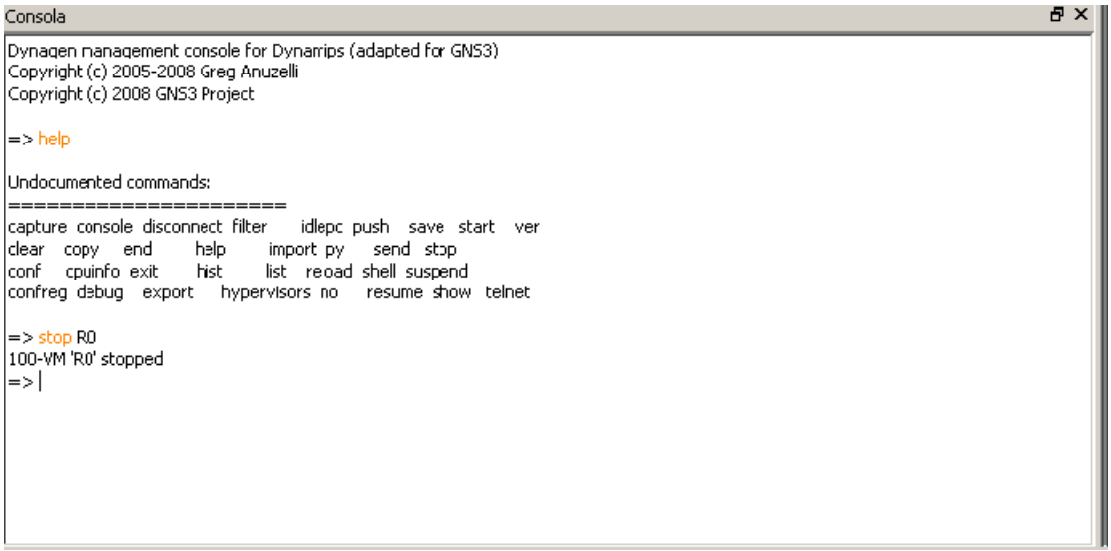
Para obtener una ayuda sobre un comando en particular escriba **help*comando*** o ***comando* ?**.

Para apagar un router virtual, utilice el comando stop. Help muestra la sintaxis: stop {/all | router1 [router2] ...}

Para detener un solo router, type**stop *nombredelrouter*.**



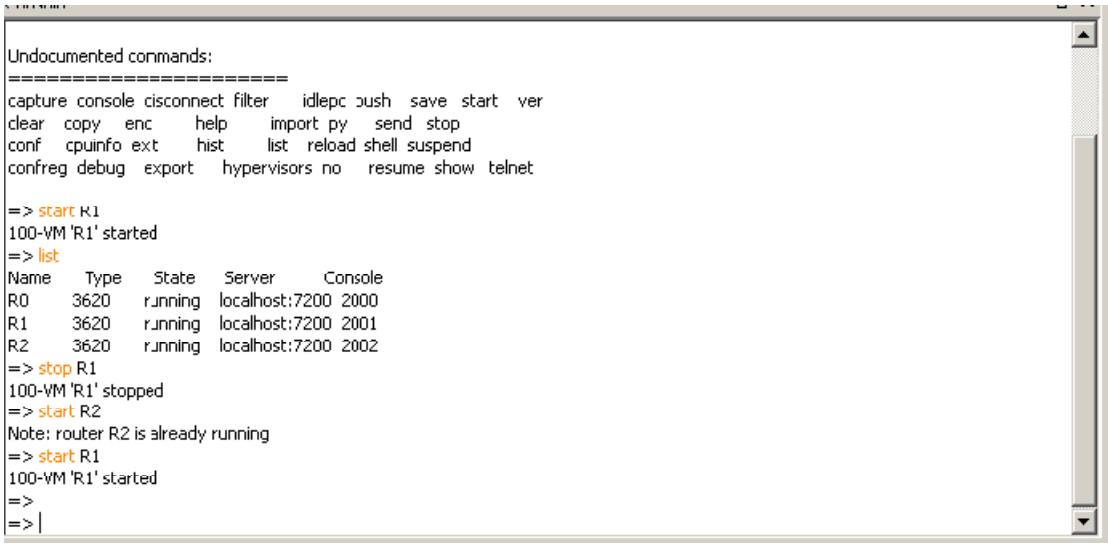
Para verificar, el routeresta detenido.



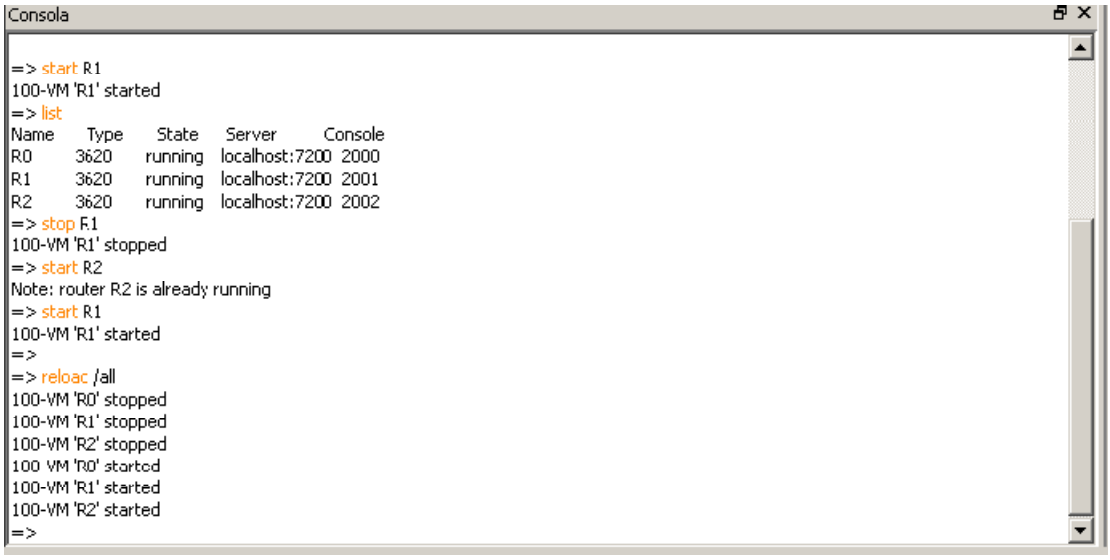
También puede informar una lista de derouters a detener, utilizar el stop /all para detener todas las instancias:

Para reiniciar R1, utilice el comando start:

Start {/all | router1 [router2] ...}



El comando de IOS reload no esta soportado por Dynamips en los routersvirtuales. Por eso puede usar el comando **reload**de la consola. Realiza un stop ya continuación un start. Para reiniciar todos los routers del laboratorio, utilice alcomando **reload /all.**

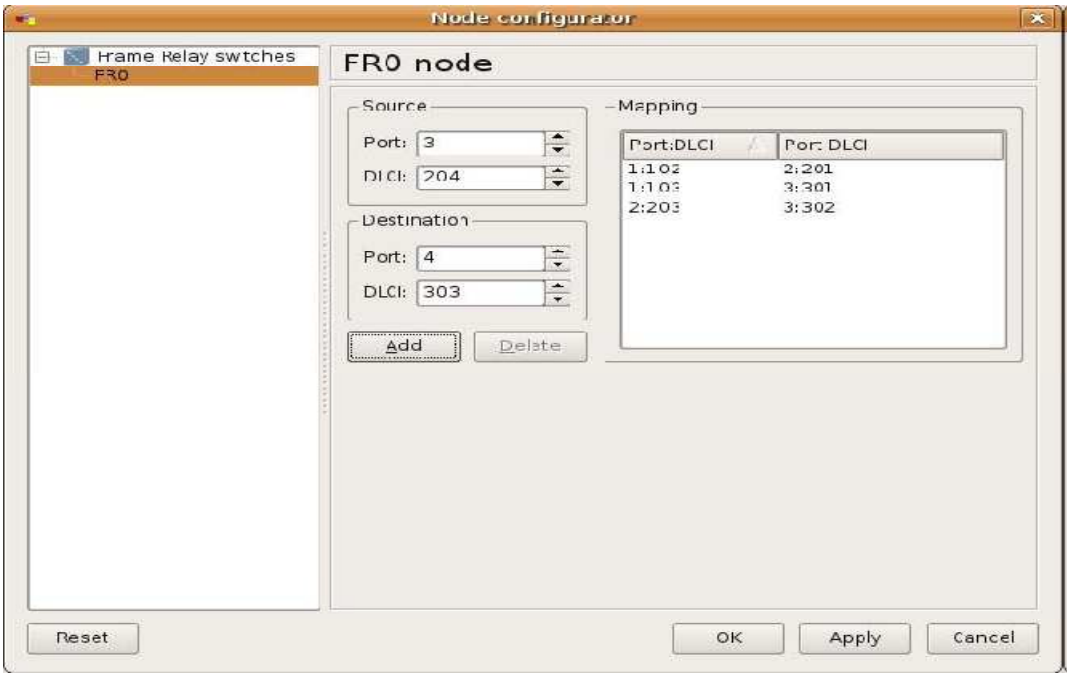


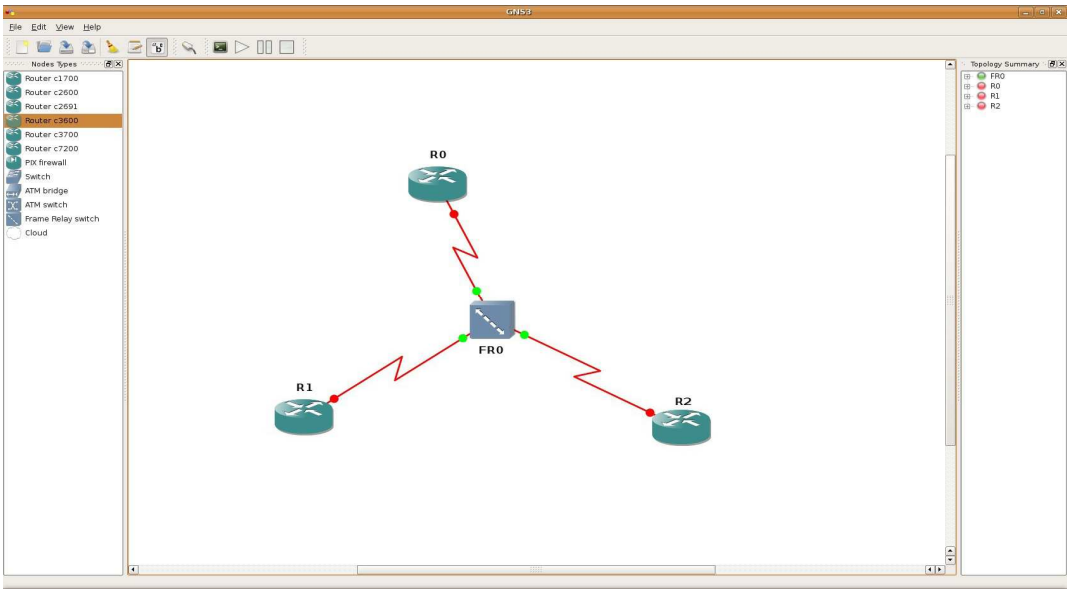
Los comandos suspend y resume tienen una sintaxis similar, pero solo suspenden temporariamente el funcionamiento de los routers.

UTILIZANDO EL DISPOSITIVO FRAME RELAY

Dynamips (consecuentemente GNS3) provee soporte para un integrado switch frameRelay.

Visualizando el labframeRelay:





Hemos conectado las interfaces seriales del router a los puertos 1, 2, y 3, respectivamente a un switchFrameRelay nombrado “F0”.

Por medio del configurador de Nodos hemos asignado un DLCI local 102 al puerto 1, que se corresponde con el DLCI de 201 al puerto 2. Las dos entradas restantes están configuradas en forma similar, por ello creando una configuración de malla completa de PVC’s entre los tres routers. (103 <->301, y 201 <-> 302).

Nota: El switchFrameRelay emulado por Dynamips utiliza LMI tipo ANSI Annex D, y no Cisco.

Cuando lanzamos el labveremos lo siguiente:

El switchFrameRelay F0 está en la lista, pero usted no podrá detenerlo, suspenderlo o continuarlo como lo hace con otros routers virtuales.

El switch ATM puede ser configurado de la misma manera.