ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE LA INFRAESTRUCTURA DE RED PARA UN MIEMBRO TIPO DE CEDIA Y PLANTEAMIENTO DE UNA ALTERNATIVA DE CONECTIVIDAD ENTRE DOS MIEMBROS

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

LUIS FELIPE MACHADO REDROBÁN

luis.fem@gmail.com

SILVIA DIANA MARTÍNEZ MOSQUERA

dianitamart@hotmail.com

DIRECTOR: ING. FERNANDO FLORES

fflores@fie.epn.edu.ec

Quito, Enero 2008

DECLARACIÓN

Nosotros, Luis Felipe Machado Redrobán Silvia Diana Martínez Mosquera, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____ _____

Luis Felipe Machado Redrobán Silvia Diana Martínez Mosquera

CERTIFICACIÓN

Certifico que el presente Proyecto de Titulación fue desarrollado por Luis Felipe Machado Redrobán y Silvia Diana Martínez Mosquera, bajo mi supervisión.

_____

Ing. Fernando Flores

DIRECTOR DEL PROYECTO

AGRADECIMIENTO

Agradezco a DIOS, a mis padres y a todos quienes han sido parte fundamental de mi vida, ya que con su apoyo y comprensión he logrado alcanzar mis metas.

Luis Machado

AGRADECIMIENTO

Agradezco primeramente a Dios, por bendecirme con la vida y la salud a mi y a todos quienes me apoyaron incondicionalmente para la obtención de un título profesional.

Agradezco a mi madre Rosa Mosquera, por darme siempre lo que no tenía y no lo que le sobraba, por su fuerza, por su entrega sin medida, por la inspiración que me dio durante todos los años de estudio.

Agradezco a mi hermana Erika Martínez, por su comprensión, por su compañía, por toda su ayuda sin esperar nada a cambio.

A mi esposo Carlos Castillo, quien con su amor y su apoyo me impulsó a alcanzar la meta de mi vida estudiantil.

A mi hija Victoria, tan pura e inocente le dio una razón primordial a mi existir y a la lucha por ser mejor cada día.

A toda mi familia, cada integrante fue parte fundamental del estímulo de constancia y tenacidad.

A mi compañero de tesis, un amigo de verdad, por su paciencia y su colaboración total para la culminación de este proyecto.

Y a nuestro director de proyecto de titulación el Ing. Fernando Flores, por guiarnos siempre con visión en nuestro porvenir tanto profesional como humano.

Silvia Martínez

DEDICATORIA

Dedico el presente trabajo a mi madre GLORIA, ya que con su infinito amor he logrado superar todos los obstáculos que se me han presentado.

Luis Machado

DEDICATORIA

Dedico este proyecto de titulación a todos quienes tienen un sueño y lo creen inalcanzable, ésta es una muestra de que quien confía en Dios y lo tiene presente en todas las actividades de su vida, es rodeado de personas que en conjunto hacen posible realizar nuestros anhelos.

Esas personas en mi caso fueron mi madre, mi hermana, mi esposo, mi hija, mis abuelitos, mis tias, mis amigos, a ellos mi total admiración y gratitud.

Silvia Martínez

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ECUACIONES

RESUMEN

El presente proyecto de titulación realiza un estudio de las principales aplicaciones de las redes avanzadas y sus protocolos, cómo podrían éstas adecuarse a la realidad de la red avanzada ecuatoriana a través del diseño de la infraestructura de red para un miembro tipo y se plantea además una alternativa de conectividad entre dos miembros en caso de perder el acceso a la red dedicada.

En el primer capítulo se presenta en forma detallada cómo se encuentra estructurada la red avanzada ecuatoriana tanto en su parte física como organizacional. Se muestra el listado de los miembros actuales del Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado, las capacidades contratadas, las características de sus enlaces, los proyectos acordados, el aporte económico de cada uno, entre otros detalles.

Se realiza además un análisis comparativo con dos redes avanzadas latinoamericanas como son la Red Universitaria Nacional de Chile y la Red Nacional de Enseñanza e Investigación de Brasil, con estos datos se presenta al final un análisis de las fortalezas, oportunidades, debilidades y amenazas de la institución.

En el segundo capítulo se estudia el funcionamiento y utilización de las principales aplicaciones de las redes avanzadas, así tenemos las bibliotecas digitales, teleinmersión, laboratorios virtuales, telemedicina, VRSV, simulación distribuida, *learningware* o *software* de aprendizaje y una nueva aplicación como la astronomía.

Se estudia también el funcionamiento de los principales protocolos y tecnologías utilizadas por las aplicaciones, así tenemos la tecnología *multicast*, el protocolo Ipv6, el estándar H.323, entre otros.

En el tercer capítulo se analiza primeramente el tráfico generado por las principales aplicaciones de las redes avanzadas, posteriormente se describen los protocolos y se realiza el cálculo de la capacidad del enlace de datos, necesarios para la utilización de las aplicaciones.

Luego de analizada toda esta información se plantea el diseño de la infraestructura de red para un miembro tipo, se describe la topología física de la red, las características de los equipos de interconexión a utilizarse, el cableado estructurado, el *software* y el presupuesto para la implementación del diseño con los equipos sugeridos, tomando en cuenta los requisitos mínimos y los costos promedios del mercado.

En el cuarto capítulo se plantea una alternativa de conectividad entre dos miembros de la red avanzada ecuatoriana, el momento que pierdan conexión con la red dedicada. En el planteamiento constan los protocolos, las tecnologías, las configuraciones básicas de los servicios en los equipos, el *software* necesario, las redes a las que se debe acceder y el procedimiento de obtención de membresías, los requisitos técnicos para los miembros y finalmente el presupuesto para la implementación de la propuesta.

En el quinto capítulo constan las respectivas conclusiones y recomendaciones del proyecto de titulación.

Además constan 2 anexos, el primero correspondiente a las características del equipo recomendado en el diseño y el segundo a la configuración de protocolos de enrutamiento del *software* propuesto como alternativa.

PRESENTACIÓN

La capacidad de comunicación en la actualidad marca las riendas del progreso y el desarrollo, pues a través de ella se puede compartir grandes cantidades de información y de todo tipo. La comunicación abre fronteras a la educación, comercio, industria, etc.

Las universidades al ser el pilar fundamental en el desarrollo de un país, deben estar altamente equipadas y principalmente colaborar entre ellas por un fin común que es el de investigación.

Existe en la actualidad proyectos de colaboración entre las universidades y una infraestructura de red que une a las mismas en forma privada, este proyecto existe a nivel mundial y son las llamadas **redes avanzadas**.

En nuestro país existe una red avanzada, sin embargo, está siendo subutilizada, por consiguiente, se plantea el siguiente proyecto, el mismo que permitirá al lector entender y conocer las aplicaciones existentes de las redes avanzadas y el modo de acceder a ellas.

Se espera que el proyecto brinde una pauta y genere la necesidad de inventiva capaz de motivar al lector, no solo a conocer las redes avanzadas sino a desarrollar servicios para las mismas y compartirlos con el mundo, ya que han sido desarrolladas para aquello.

1 ESTUDIO DE LAS REDES AVANZADAS EN EL ECUADOR

1.1 ESTUDIO DE LA ESTRUCTURA ACTUAL DE CEDIA [1] [2]

CEDIA (Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado) es una red de investigación y educación miembro de la red CLARA (Consorcio Latino Americano de Redes Avanzadas), a través de la cual se enlaza a las redes académicas avanzadas de los Estados Unidos INTERNET2, y de Europa GÉANT2, proyectándose a tener un enlace con Asia.

CLARA a través del proyecto ALICE (América Latina Interconectada con Europa) se logra enlazar a la red GÉANT2, para esto, la Comunidad Europea asignó 12,5 millones de euros, lo cual representó el 80% del financiamiento requerido para su construcción y operación hasta mayo del 2007, el 20% restante corrió por cuenta de sus socios latinoamericanos, esta cantidad no fue dividida en partes iguales sino en función de la capacidad contratada, Ecuador tiene contratado 10 Mbps.

El enlace de CLARA con GÉANT2 se establece entre el nodo de Sao Paulo (Brasil) y Madrid (España) a 622 Mbps y el enlace de CLARA con INTERNET2 se establece entre el nodo de Tijuana (México) y Los Angeles (Estados Unidos) a 155 Mbps.

La figura 1.1 muestra la topología de la red Clara, con la cual se entenderá como se encuentra enlazado Ecuador con las demás redes a nivel de América. Ecuador se une a CLARA desde Punta Carnero (costa) hasta Arica en Chile a través del Cable Panamericano.

1.1.1 MIEMBROS

Los miembros de CEDIA se clasifican en:

a) Asociados Académicos de Investigación y Desarrollo Científico
b) Asociados Estratégicos
c) Adherentes
d) Honorarios

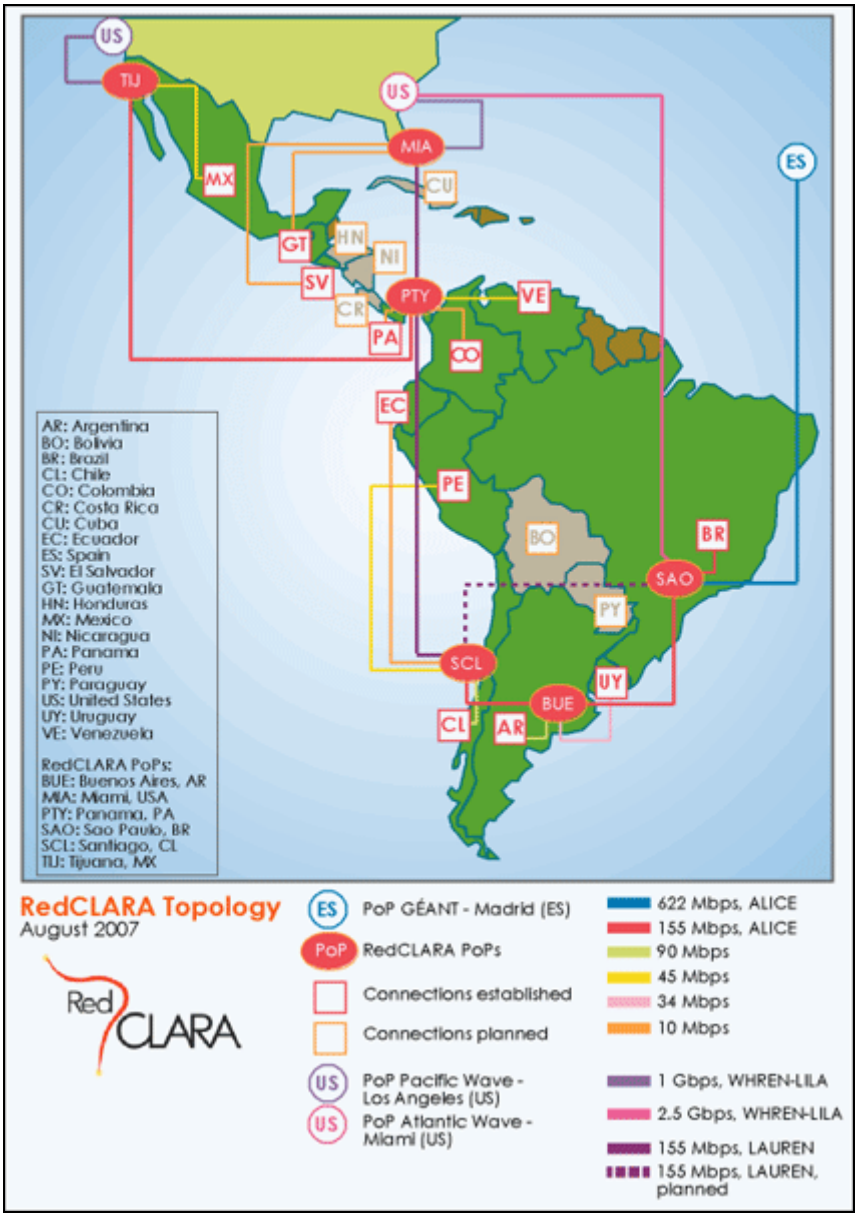


Figura 1.1 Red Clara [2]

1.1.1.1 Asociados Académicos de Investigación y Desarrollo Científico

Pertenecen a este grupo las Universidades y Escuelas Politécnicas, Centros de Investigación y Desarrollo Científico que cumplen con lo siguiente:

- Haber obtenido aprobación de membresía por parte del Directorio previo informe favorable de la Comisión de Membresías.
- Poseer un memorando de compromisos en los que consten sus derechos y obligaciones.
- A nivel de infraestructura, poseer un nodo de computación con alta capacidad de transmisión.
- Compromiso de promover la interconexión con otros nodos de la red nacional e internacional.
- Hacer uso y desarrollo de aplicaciones educativas a nivel informático.
- Destinar recursos tanto humanos como financieros en el desarrollo y cumplimiento de lo anteriormente mencionado.

1.1.1.2 Asociados Estratégicos

Pertenecen a este grupo aquellos entes que colaboren con el desarrollo, evolución y utilización de aplicaciones educativas y de tecnología avanzada, a través de un aporte económico cuyo monto será determinado por el Consejo Directivo.

Además deberán cumplir lo siguiente:

- Haber obtenido aprobación por parte de la Comisión de Membresías de acuerdo a los estatutos.
- Poseer un documento aprobado por el Directorio en el que se establezcan los derechos y obligaciones que contrae.

1.1.1.3 Adherentes

Pertenecen a este grupo las Universidades y Escuelas Politécnicas, Centros de Investigación y Desarrollo Científico que, aunque no posean un nodo de computación con alta capacidad de transmisión, colaboren con el desarrollo de aplicaciones educativas a nivel informático.

Además pertenecerán a este grupo quienes cumplan con lo siguiente:

- Haber obtenido aprobación de membresía por parte del Directorio previo informe favorable de la Comisión de Membresías.
- Poseer un documento aprobado por el Consejo Directivo en los que consten sus derechos y obligaciones.
- Poseer un documento suscrito con un Asociado Académico en el que se establezca la obligación de destinar recursos académicos adicionales para el desarrollo de aplicaciones educativas a nivel informático.
- Demostrar que se han realizado las instalaciones necesarias para la conexión al nodo de alta capacidad del Asociado Académico.

1.1.1.4 Honorarios

Pertenecen a este grupo las personas naturales o jurídicas que han prestado sus servicios a la institución y que han obtenido por lo menos las tres cuartas partes de los votos de los integrantes del Consejo Directivo.

Entre las atribuciones y deberes de los miembros honorarios se tiene:

- Asesorar al Directorio, al Presidente y al Director Ejecutivo en la búsqueda de recursos y el fortalecimiento de la institución.
- Integrar las comisiones permanentes y de trabajo.

1.1.2 MIEMBROS DE CEDIA

A la fecha Agosto del 2007, la red CEDIA se encuentra conformada por 23 miembros.

1.1.2.1 Miembros Académicos de Investigación y Desarrollo Científico

1. Escuela Superior Politécnica del Chimborazo – ESPOCH
2. Escuela Superior Politécnica del Ejército – ESPE
3. Escuela Superior Politécnica del Litoral – ESPOL
4. Escuela Politécnica Nacional – EPN
5. Instituto Nacional de Pesca – INP
6. Instituto Oceanográfico de la Armada del Ecuador – INOCAR
7. Pontificia Universidad Católica de Ibarra – PUCI
8. Pontificia Universidad Católica de Santo Domingo – PUCSD
9. Universidad Católica de Santiago de Guayaquil – UCSG
10. Universidad Central del Ecuador – UCE
11. Universidad de Cuenca – UC
12. Universidad Estatal de Milagro – UNEMI
13. Universidad Internacional del Ecuador – UIE
14. Universidad Nacional del Chimborazo – UNACH
15. Universidad Nacional de Loja – UNL
16. Universidad de San Francisco de Quito – USFQ
17. Universidad Técnica de Ambato – UTA
18. Universidad Técnica Equinoccial – UTE
19. Universidad Técnica Particular de Loja - UTPL

1.1.2.2 Miembros Estratégicos

20. Consejo Nacional de Telecomunicaciones – CONATEL
21. Empresa de Transmisión Eléctrica – TRANSELECTRIC
22. Secretaría Nacional de Ciencia y Tecnología – SENACYT

1.1.2.3 Miembros Honorarios

23. Steve Huter, Universidad Oregon, quien donó 2 enrutadores para los nodos principales.

1.1.3 PROYECTOS

CEDIA se encuentra en la actualidad gestionando la ejecución de proyectos que se han venido planteando en las distintas reuniones del directorio y los representantes de las instituciones miembros.

Un claro ejemplo es la gestión para la subida de la capacidad en los accesos de última milla de los miembros, las cuales, anteriormente eran como mínimo de 384 kbps y en la actualidad el mínimo es 1 Mbps, manteniendo los costos anteriores.

Esta propuesta fue expuesta a Telconet por el directorio de CEDIA debido a la falta de garantía en la ejecución de las aplicaciones de las redes avanzadas, en el caso mayor utilizado, las videoconferencias.

Entre los proyectos que tiene en la mira actualmente CEDIA están:

- Fomentar la creación y gestionar la consecución de fondos a por lo menos 2 redes de científicos ecuatorianos, para la ejecución de sus proyectos.

Las propuestas fueron presentadas por los respectivos grupos de trabajo a representantes de CLARA y a los fondos CEREP (Cuenta de Reactivación Productiva y Social, Desarrollo Científico -Tecnológico y Estabilidad Fiscal).

Los grupos de trabajo formados en la actualidad son:

a) **Grupo de Materiales y Nanotecnología** que tiene como contraparte internacional a Estados Unidos y Bélgica.

b) **Grupo de Biotecnología** que tiene como contraparte internacional a Alemania y Bélgica.

c) **Grupo de Tecnologías de Información** que tiene como contraparte internacional a Estados Unidos.

Entre las propuestas del Grupo de Tecnologías de Información se tiene:

1. Proporcionar a instituciones académicas y de investigación, un arreglo de cómputo distribuido de alto rendimiento conformado por 2 centros de computación conectados mediante la red avanzada, al arreglo accederán las instituciones a través de sus propios recursos tecnológicos.

- Crear la primera troncal académica a través de la red de fibra óptica de Transelectric, con lo cual se obtendrá un enlace de 45 Mbps aproximadamente. Para llevarlo a cabo el Grupo de Tecnologías de Información definirá los requerimientos técnicos de los miembros de CEDIA para la última milla.

- Creación de un repositorio de objetos de aprendizaje en base a código abierto, el cual estará orientado a estudiantes de nivel superior.

- Permitir que a través de la red avanzada se realicen experimentos remotos enfocados a 3 áreas del conocimiento: Física, Electrónica y Mecánica.

2. Resolver la conexión de los nodos de CEDIA a través de Transelectric.

- De realizarse la conexión entre los nodos CEDIA de Guayaquil y Quito

a través de la infraestructura de Transelectric, los costos serían los siguientes:

Servicio de Conexión Nodos CEDIA Guayaquil y Quito por medio de la infraestructura de TRANSELECTRIC			
	Costo de Instalación	Costo Mensual	Costo Total el primer año
Última milla urbana por medio de la red de Telconet, utilizando una capacidad de 45 Mbps (DS3)	$ 2 200,00	$ 7 000,00	$ 86 200,00

Tabla 1.1 Costos [1]

Por lo tanto, el primer año se pagaría en total $ 86 200 y los siguientes años $ 84 000.

- Físicamente los enlaces quedarían establecidos entre Guayaquil y Quito a 45 Mbps mediante fibra óptica.

CONEXIÓN GUAYAQUIL	**CONEXIÓN QUITO**
Punto A: Transelectric Policentro Gye	Punto A: Transelectric Edif. administrativo
Punto B: Backbone de Telconet Gye	Punto B: Backbone de Telconet Uio
Capacidad: 45 Mbps	Capacidad: 45 Mbps

Tabla 1.2 Características de conexión [1]

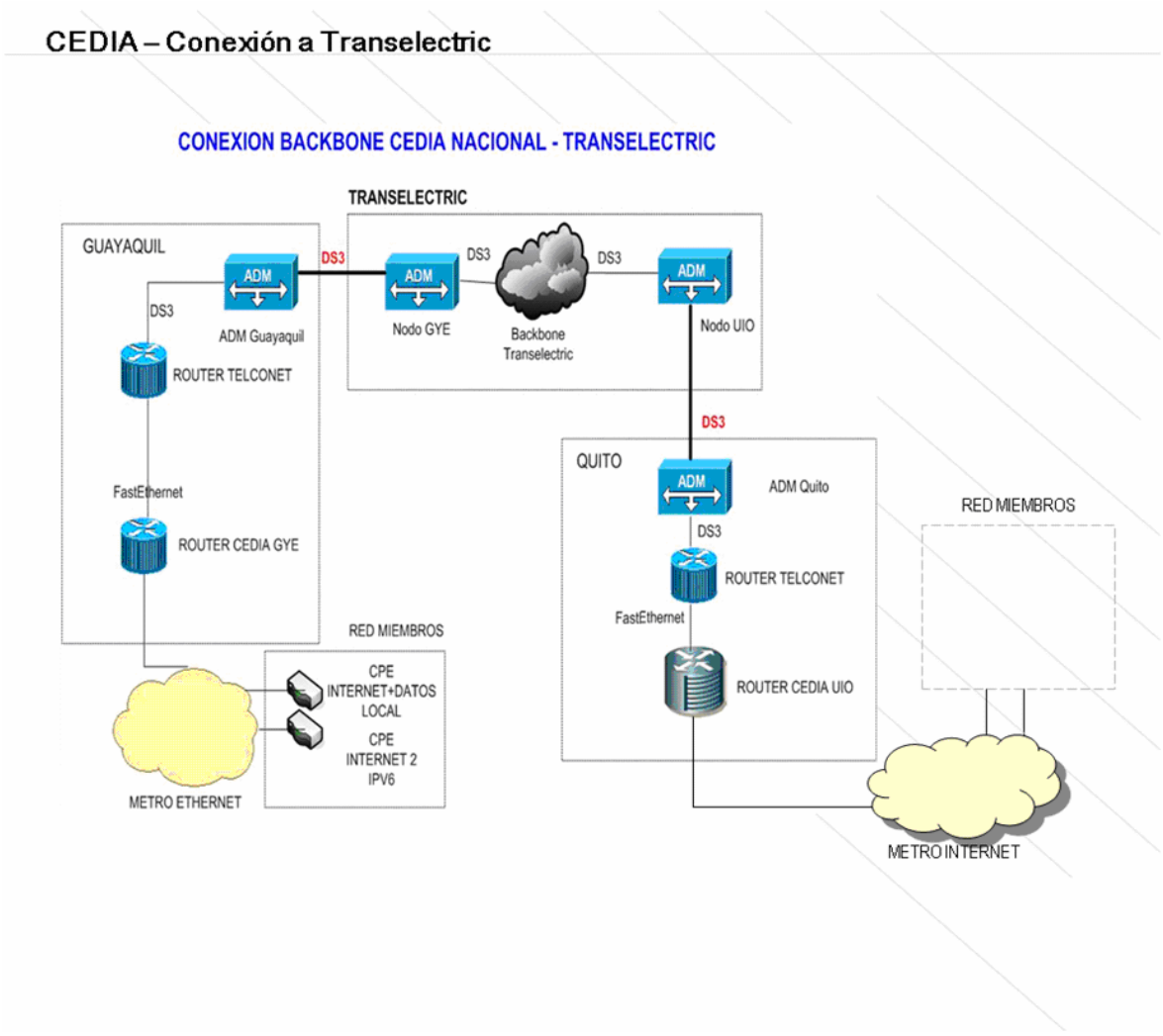


Figura 1.2 Conexión a Transelectric [1]

3. Incorporar a la organización por lo menos a 5 miembros académicos y 1 miembro estratégico.

Al inicio se había planteado el no aceptar más miembros a CEDIA debido a la escasa capacidad de 10 Mbps contratada para la unión internacional con CLARA, pero al momento se decidió por planes estratégicos el recibir nuevas solicitudes de universidades que deseen pertenecer a la red avanzada.

Las universidades de las que se ha recibido la solicitud a la fecha actual son:

- Universidad Técnica del Norte – Ibarra
- Universidad Estatal de Bolívar – Guaranda
- Universidad Tecnológica San Antonio – Machala
- Universidad Estatal de Guayaquil
- Universidad Laica Eloy Alfaro de Manabí

Y las instituciones que pasarían a ser miembros estratégicos:

- Empresa GLOBATEL – A informe de la Comisión Técnica.
- Empresa EASYNET – A informe de la Comisión Técnica.

A la fecha actual, la universidad de Bolívar, luego de la aprobación de membresía por parte del Directorio de CEDIA, confirmó su unión a la red avanzada, Telconet realizó la inspección de las instalaciones y envió un informe de la instalación de fibra.

4. Desarrollar un taller internacional de alto perfil con la participación de todos los miembros de CEDIA, las organizaciones nacionales relacionadas con el desarrollo, tomadores de decisiones del gobierno y otras universidades.

Hasta el momento se han realizado varios talleres:

- Del 16 al 20 de Enero del 2006 se llevó a cabo el III Taller Internacional de redes avanzadas con sede en la universidad de Cuenca.

- El 11 de Enero del 2007 se llevó a cabo un Taller a nivel nacional de redes avanzadas en el Hotel Hampton en Guayaquil.

- El 12 de Enero del 2007 se realizó otro Taller a nivel nacional de redes avanzadas en el Hotel Nu House en Guayaquil.

5. Desarrollar una pasantía de por lo menos dos técnicos ecuatorianos en una organización internacional relacionada con las redes avanzadas, operación y seguridades en redes.

A nivel internacional, la Universidad de Oregon ha ofrecido para 1 o 2 ingenieros de CEDIA una pasantía por 2 a 3 semanas para formación en:

- Aplicaciones en BGP (*Border Gateway Protocol*), IPv6, IPv4 *Multicast*, MPLS (*Multi Protocol Label Switching*).

- Operaciones y administración tipo NOC (*Network Operations Center*), NEG (*Network Engineering Group*).

A nivel nacional, la UTPL y la ESPOL han ofrecido para 1 o 2 ingenieros en CEDIA entrenamiento acerca de:

- Aplicaciones en IPv6, IPv4 *multicast*, Isabel – videoconferencia.
- Planes de desarrollo informático.

6. Poner en operación el servicio de telefonía sobre IP entre todos los miembros de CEDIA.

Una alternativa propuesta por el directorio es el uso de la aplicación Skype para la comunicación telefónica entre los miembros de CEDIA, lo cual ofrecería muchas

ventajas entre ellas el cero costo en llamadas entre los miembros, pero como gran desventaja el no poder comunicarse a teléfonos convencionales o celulares.

Otra de las alternativas propuestas es el de usar un servidor de VoIP (Voz sobre IP), el cual estará conectado a dos interfaces de red, una a Internet comercial y otra a la red CEDIA, de modo que pueda ser usado por los miembros a través del Internet comercial o a través de la red avanzada.

La implementación de dicho servidor tendría un costo de 3000 USD, valor que sería donado, pero para el uso del mismo cada institución requerirá obtener un teléfono IP cuyo valor es de 95 USD aproximadamente.

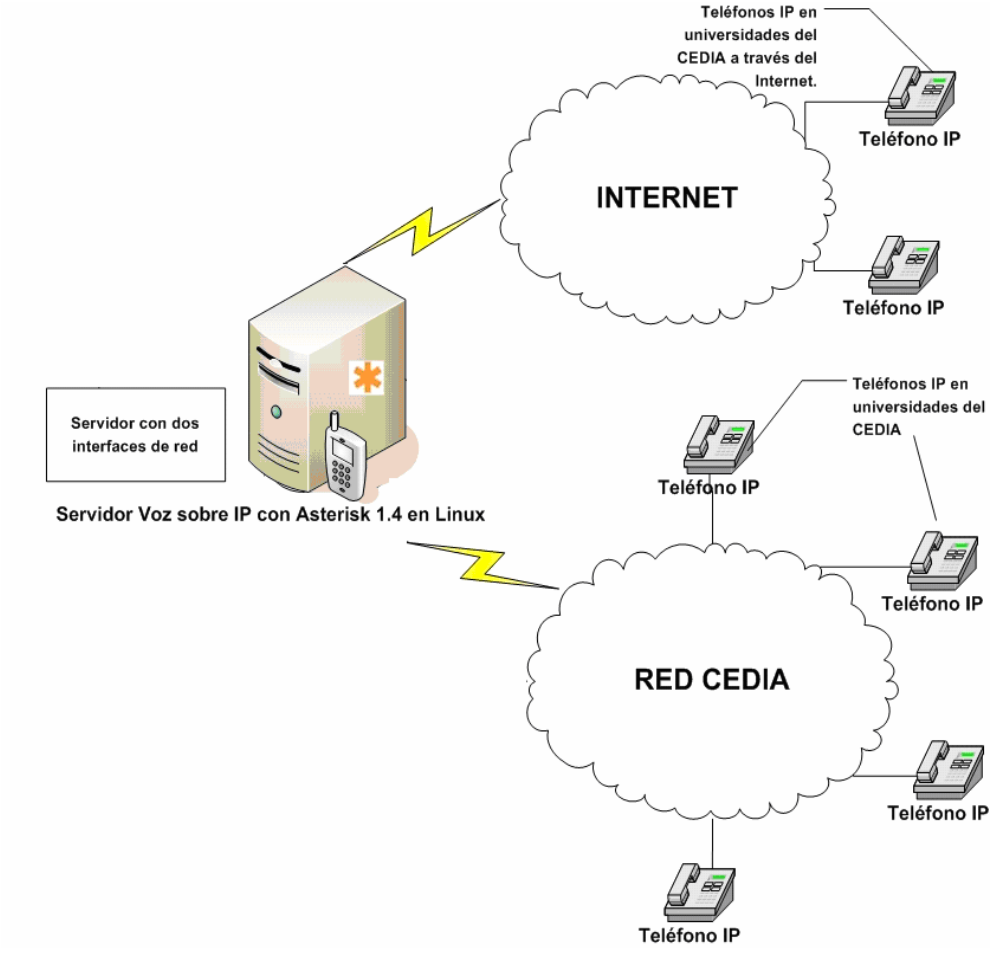


Figura 1.3 Esquema de conexión de voz

7. Actualizar la base de datos de los grupos de científicos ecuatorianos que trabajan en las instituciones de CEDIA.

8. Elaboración de la propuesta del proyecto CEDIA para la búsqueda de financiamiento no reembolsable con organismos internacionales. Se han generado hasta el momento dos documentos:

- Propuesta de desarrollo de CEDIA.
- Perfiles de proyectos.

9. Desarrollar un taller para la elaboración del plan estratégico de CEDIA.

Dicho plan deberá contener:

- El levantamiento de información y diagnóstico.
- Definición del marco del plan estratégico.
- Matrices FODA.
- Definición de la estrategia.
- Definición de las metas y medios.

La elaboración del plan estratégico tendría un costo de 5000 USD sin incluir impuestos, los cuales deberán ser cancelados, el 60% al inicio y el 40% restante a la entrega del plan.

10. Incorporación a las primeras jornadas sobre redes avanzadas en la segunda reunión de directorio, el segundo semestre del año 2007.

11. Hacer el seguimiento de la interconexión de las otras ciudades a la troncal Quito – Guayaquil en la infraestructura de Transelectric.

A través de un convenio firmado con Transelectric el 22 de septiembre del 2005, al ser éste un miembro estratégico de CEDIA, se pretende unir a los miembros de CEDIA a nivel nacional a través de la red de fibra óptica de Transelectric, el cual provee una capacidad de 45 Mbps entre los nodos de Quito y Guayaquil.

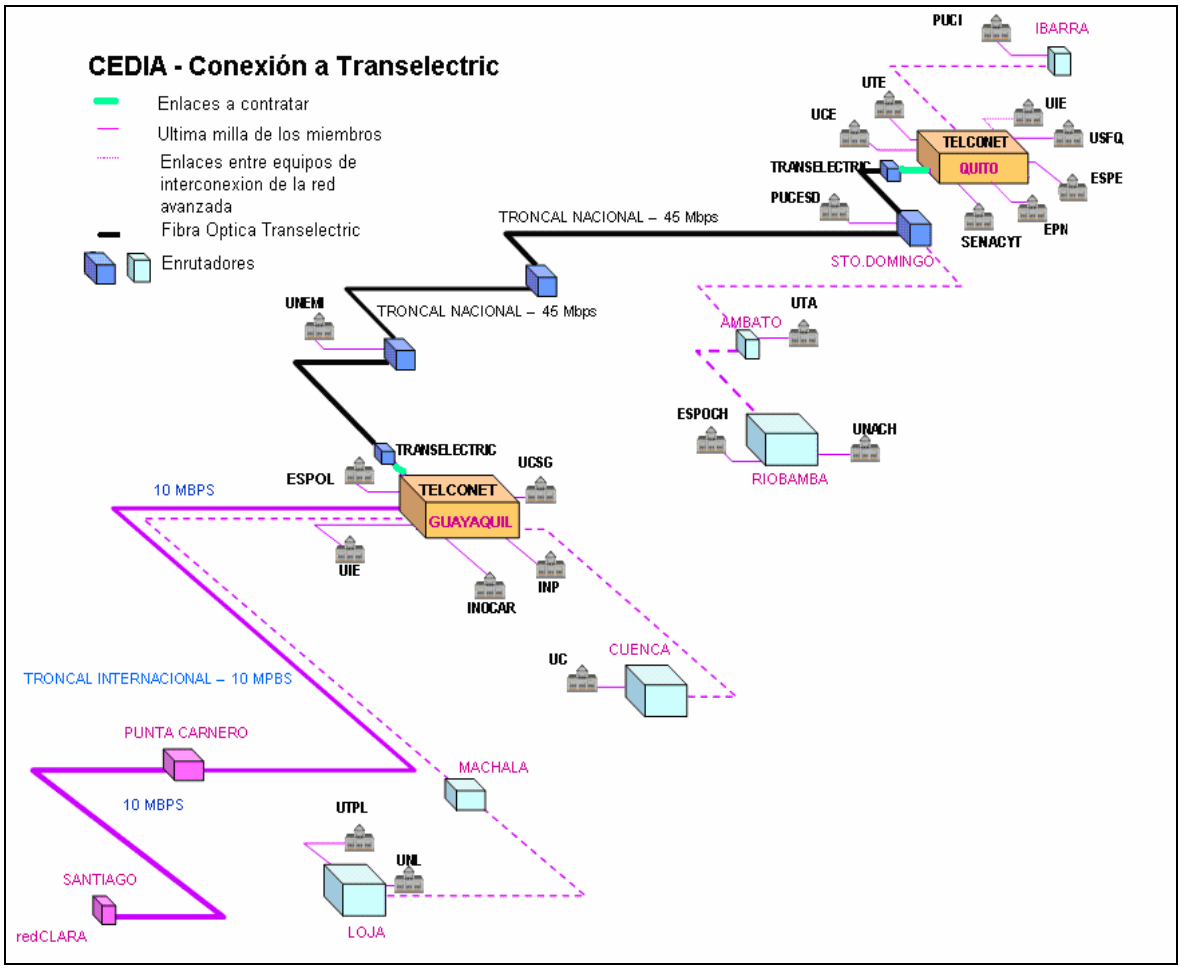


Figura 1.4 Proyecto Transelectric [1]

La limitante de este proyecto es el requisito de tener una propia infraestructura con respecto a los nodos de Quito y Guayaquil, con lo cual no cuenta CEDIA en la actualidad, aunque la idea desde un principio fue que los nodos principales se

encuentren en Guayaquil en la Escuela Politécnica del Litoral y en Quito en la Escuela Politécnica Nacional.

Además la conexión entre los nodos principales y los nodos de Transelectric significan un gasto adicional de 7000 dólares mensuales, costo que deberá ser asumido por todos los miembros de CEDIA.

1.2 ESTUDIO DE LA ESTRUCTURA ACTUAL DE LOS PRINCIPALES NODOS DE CEDIA

1.2.1 ESTRUCTURA DE RED DE LA ESCUELA POLITÉCNICA NACIONAL

En un principio CEDIA tuvo como objetivo hacer de la Escuela Politécnica Nacional y la Escuela Politécnica del Litoral, los nodos principales de la red avanzada a nivel nacional y que sean éstas quienes unan a los demás miembros a través de su infraestructura, pero debido a la falta de recursos tanto técnicos como humanos, este planteamiento no fue ejecutado y en la actualidad los nodos se unen a través de Telconet.

Actualmente la Escuela Politécnica Nacional se encuentra unida a CEDIA a través de un enlace de 1.564 Mbps de fibra óptica entre sus instalaciones y Telconet.

Para acceder a los recursos de la red avanzada y del Internet comercial la Escuela Politécnica Nacional ha adquirido recientemente un enrutador que le permite, entre otras características, utilizar BGP y MPLS.

El enrutador con el que primeramente se conectaba la EPN con la red avanzada era un Cisco 4500 de 6 puertos de 10 Mbps y 1 puerto de 100 Mbps, el cual se encuentra en la actualidad fuera de mercado.

Entre las principales características del enrutador Cisco 3845, adquirido recientemente por la Escuela Politécnica Nacional, se tiene:

- Posee 6 interfaces de red, 2 de ellas trabajan a 1 Gbps, y las otras 4 a 10/100 Mbps.
- Módulo de alta densidad analógica y digital para voz y fax.
- Soporte VPN (*Virtual Public Network*).
- Puede utilizarse como *gateway* LMR (*Land Mobile Radio*).
- Posee un soporte reforzado para conferencia.
- Provee seguridad en la red.
- Discriminación de tráfico por una misma interfaz de red.
- Multiplexación de datos y voz.
- Posee un módulo EtherSwitch, el cual, soporta el estándar 802.1p, priorización de tráfico y filtrado *multicast* a nivel de capa 2.
- Posee un módulo integrado que permite reconocer usuarios, sus dispositivos y demás funciones en la red, en este paso se realiza autenticación para evitar que código malicioso pueda ocasionar daños.
- Soporte para la interconexión de equipos telefónicos , tales como PBXs (*Private Branch Exchanges),* teléfonos analógicos y fax.
- Soporte para comunicaciones inalámbricas.
- A través de medios de autenticación y encriptación permite garantizar conversaciones de voz seguras.

Actualmente la estructura de red de la Escuela Politécnica Nacional se encuentra conformada por:

- Un enrutador Cisco 3845, el cual posee 6 interfaces de red, 2 de ellas de 1 Gbps conectadas una al Internet comercial y otra a la red avanzada , 3 interfaces de 10/100 Mbps conectadas, una al servidor NAT (*Network Address Translation*), otra al *firewall* del servidor SAEW (Sistema de Administración Estudiantil *Web*) y la otra a los servidores de correo y DNS (*Domain Name System*), servidor de bases de datos y servidor *web*.

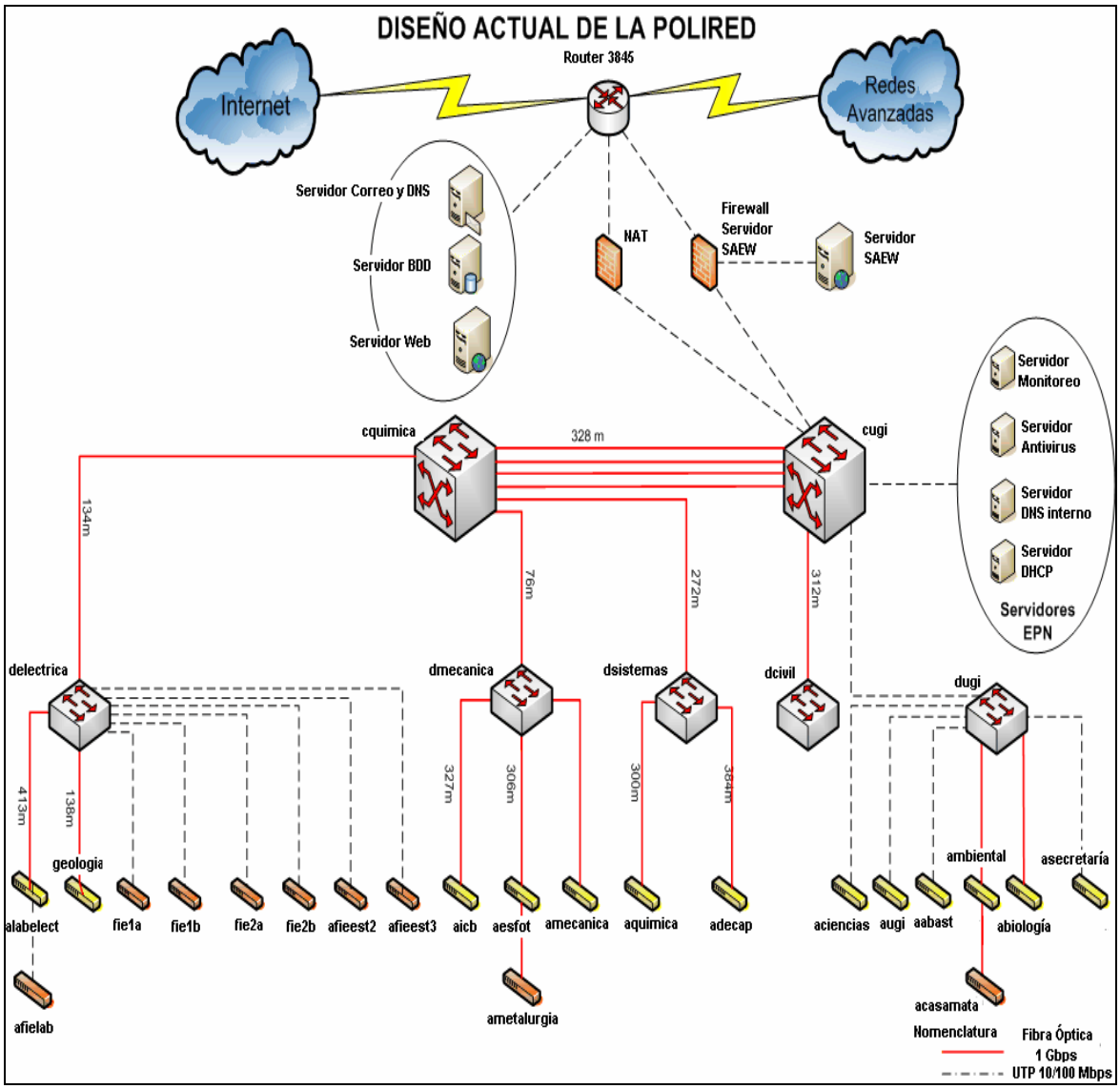


Figura 1.5 Diagrama de red EPN

- Dos *switches* de *core* ubicados uno en la UGI (Unidad de Gestión de la Información) y otro en el edificio de Ingeniería Eléctrica. Entre los *swtiches* de *core* existen 4 hilos de fibra óptica de 1 Gbps cada uno.

- Cinco *switches* de distribución ubicados en las facultades de Ingeniería Eléctrica y Electrónica, Ingeniería Mecánica, Ingeniería en Sistemas, Ingeniería Civil y la UGI.

- Veinte y dos *switches* de acceso, ubicados en las diferentes facultades y departamentos existentes.

La tecnología de red utilizada en el *backbone* actualmente es *Gigabit Ethernet*.

1.2.2 ESTRUCTURA DE RED DE LA ESCUELA POLITÉCNICA DEL LITORAL

Actualmente la Escuela Politécnica del Litoral cuenta con varios equipos tanto para el manejo de su red de área local como de su red de área extendida.

A nivel interno cuenta con un *backbone* conformado por las máquinas correspondientes al personal, las cuales se encuentran detrás de un *firewall* en *hardware*, cuenta además con servidores *proxy* que permiten controlar el acceso a sitios no permitidos y el acceso al Internet.

Cuentan con una zona desmilitarizada (DMZ) en la cual se encuentra un servidor de correo y DNS bajo el sistema operativo Linux y un servidor *web* bajo el sistema operativo Windows.

En el NOC cuentan con 2 equipos para el monitoreo de la red de datos de la Escuela Politécnica del Litoral, uno bajo el sistema operativo Linux y otro bajo Sun Solaris.

Los equipos del área CSI (*Customer Service Inquiry*) son exclusivos para servicios internos de la institución, es decir, únicamente para la Intranet, ya que, se encuentran conformados por servidores de bases de datos.

Para la conexión con el Internet Comercial, la universidad cuenta con un enrutador Cisco 2821 propiedad de la ESPOL.

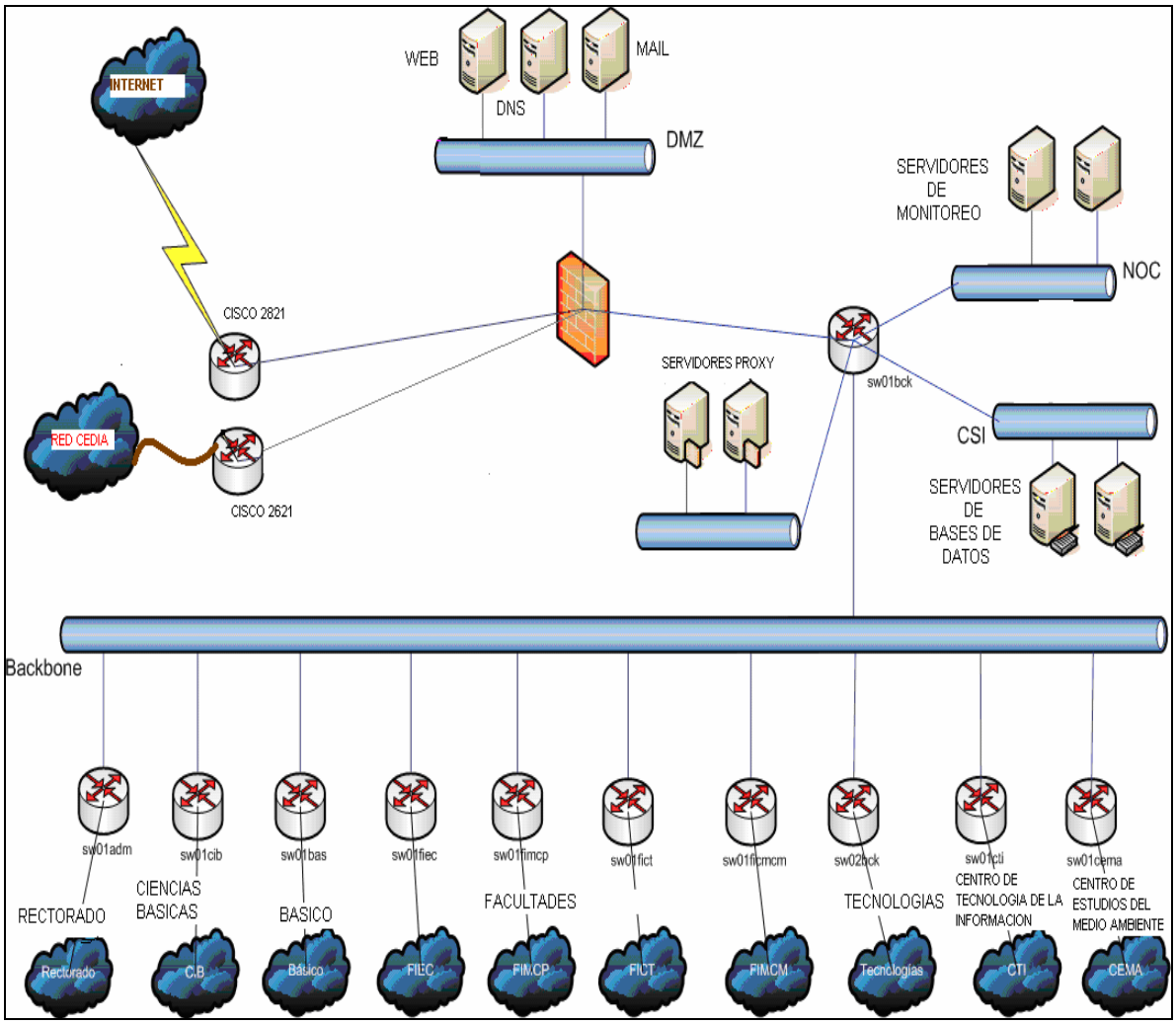


Figura 1.6 Diagrama de red ESPOL [1]

Para la conexión con la Red avanzada Telconet provee de un enrutador Cisco 2621 por el momento, ya que, están por proveer de una nueva serie.

La ESPOL tiene contratados 2.314 Mbps de capacidad para la red avanzada.

La tecnología de red utilizada en el *backone* es *Gigabit Ethernet*.

1.3 ESTUDIO DE LA CONEXIÓN DE LOS AFILIADOS DE CEDIA CON SUS NODOS PRINCIPALES [1]

Los nodos principales se encuentran en Telconet Quito y Guayaquil.

CEDIA en la actualidad cuenta con un único nodo físico que se encuentra en Telconet Guayaquil, ya que, en Quito se simula un nodo mediante un enrutador a través de túneles y VPNs (Redes Virtuales Privadas).

El equipo que se encuentra actualmente en las instalaciones de Telconet en Guayaquil es un *enrutador* CISCO 7500, el cual fue donado por la Universidad de Oregon.

Al principio de la conformación de la red CEDIA se acordó que los nodos principales se encontrarían en Guayaquil en la Escuela Politécnica del Litoral y en Quito en la Escuela Politécnica Nacional, este planteamiento no se ha concretado.

La conexión entre los nodos de Quito y Guayaquil se realiza mediante la fibra óptica de Telconet a 20 Mbps.

El enrutador que Telconet asigna a los miembros para el acceso a la red avanzada es un Cisco 1811, a excepción de aquellos que posean equipos propios como por ejemplo la Escuela Politécnica Nacional y la Escuela Politécnica del Litoral.

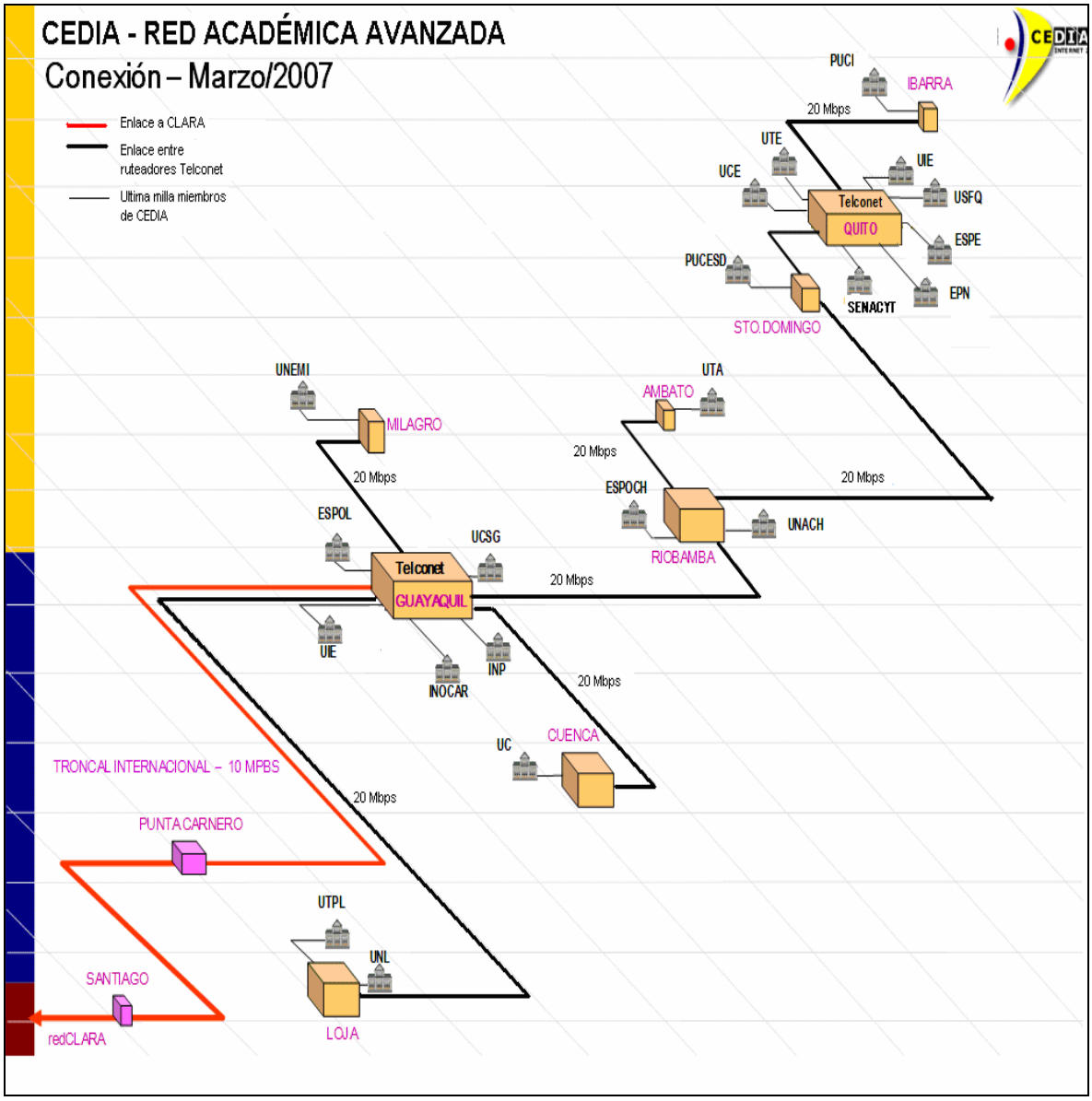


Figura 1.7 *Backbone* de CEDIA [1]

Todos los miembros se unen a los nodos principales o adherentes mediante fibra óptica a excepción de los miembros encontrados en Chimborazo, Imbabura y Loja, los cuales se unen vía microonda.

1.3.1 CAPACIDADES DE LOS ENLACES DE CADA MIEMBRO DE CEDIA

Los miembros de CEDIA, a excepción de aquellos que tienen enlaces vía microonda, poseen 2 enlaces de fibra óptica contratados con Telconet, uno es para el Internet comercial y otro para la red avanzada.

Las capacidades contratadas para el Internet comercial, por cada institución, en la actualidad son las siguientes:

INSTITUCIÓN	Capacidad contratada en Internet comercial (Kbps) Canal simétrico
Escuela Politécnica Nacional - EPN	6.040
Escuela Superior Politécnica del Ejército – ESPE	1.000
Secretaría Nacional de Ciencia y Tecnología - SENACYT	320
Universidad Central del Ecuador - UCE	5.120
Universidad San Francisco de Quito - USFQ	4.096
Universidad Técnica Equinoccial - UTE	4.683
Escuela Superior Politécnica del Chimborazo - ESPOCH	6.144
Universidad Técnica de Ambato - UTA	3.072
Universidad de Cuenca - UC	3584
Escuela Superior Politécnica del Litoral - ESPOL	14.000
Instituto Nacional de Pesca - INP	512
Instituto Oceanográfico de la Armada - INOCAR	896

Universidad Católica Santiago de Guayaquil - UCSG	2.000
Universidad Internacional del Ecuador - UIE	896
Universidad Nacional de Loja - UNL	2.560
Universidad Técnica Particular de Loja - UTPL	4.480
Pontificia Universidad Católica de Ibarra	768
Pontificia Universidad Católica de Santo Domingo	512
Universidad Nacional del Chimborazo	2.048
Universidad Estatal de Milagro	1.024

Tabla 1.3 Capacidad contratada para Internet comercial

Las capacidades contratadas para la red avanzada, por cada institución, en la actualidad son las siguientes:

INSTITUCIÓN	**Capacidad garantizada [Kbps]**	**Capacidad Adicional Máxima [Kbps]**	**Capacidad en la Troncal Nacional [Kbps] Canal simétrico**
Escuela Politécnica Nacional - EPN	994,56	569,28	1.564
Escuela Superior Politécnica del Ejército – ESPE	994,56	94,25	1.089
Secretaría Nacional de Ciencia y Tecnología – SENACYT	994,56	30,16	1.025
Universidad Central del Ecuador - UCE	994,56	482,57	1.477
Universidad San Francisco de Quito – USFQ	994,56	386,05	1.381
Universidad Técnica Equinoccial - UTE	994,56	441,38	1.436
Escuela Superior Politécnica del Chimborazo – ESPOCH	994,56	579,08	1.574

Universidad Técnica de Ambato - UTA	994,56	289,54	1.284
Universidad de Cuenca - UC	994,56	337,80	1.332
Escuela Superior Politécnica del Litoral – ESPOL	994,56	1.319,52	2.314
Instituto Nacional de Pesca - INP	994,56	48,26	1.043
Instituto Oceanográfico de la Armada – INOCAR	994,56	84,45	1.079
Universidad Católica Santiago de Guayaquil – UCSG	994,56	188,50	1.183
Universidad Internacional del Ecuador – UIDE	994,56	84,45	1.079
Universidad Nacional de Loja - UNL	994,56	241,28	1.236
Universidad Técnica Particular de Loja – UTPL	994,56	422,25	1.417
Pontificia Universidad Católica de Ibarra	994,56	72,39	1.067
Pontificia Universidad Católica de Santo Domingo	994,56	48,26	1.043
Universidad Nacional del Chimborazo	994,56	193,03	1.188
Universidad Estatal de Milagro	994,56	96,51	1.091

Tabla 1.4 Capacidad contratada para red avanzada

La capacidad mínima de conexión a la red CEDIA era de 384 Kbps, la cual no era conveniente en la actualidad ya que para ser partícipe de una videoconferencia de calidad se necesita aproximadamente 1 Mbps, según las pruebas realizadas por el departamento técnico de CEDIA. Para solventar este tipo de inconvenientes se solicitaba a Telconet un aumento en la capacidad el momento en que se va a realizar una videoconferencia.

La capacidad más alta la tenía contratada la ESPOL con 0.9 Mbps.

Actualmente se ha incrementado las capacidades a los miembros de CEDIA, para que posean como mínimo 1 Mbps y tengan garantizada una videoconferencia de calidad.

Estadísticas afirman que de los 20 Mbps que se tienen en el enlace Quito - Guayaquil, apenas se está utilizando del 3% al 5%, por lo que es iniciativa del directorio de CEDIA se utilice más la red avanzada entre los miembros académicos.

1.3.2 COSTOS

CEDIA tiene que pagar por:

Conexión Internacional

Por la conexión internacional a través del cable panamericano se paga trimestralmente 97500 euros por los 10 Mbps, de los cuales, ALICE paga el 80% y el 20% restante, es decir, 19500 euros los paga CEDIA. La contribución de ALICE es únicamente hasta Marzo de 2008, por lo que, se pretende conseguir la contribución del estado ecuatoriano para que la salida internacional sea gratuita para la red académica y además haya un aumento de 10 Mbps a 45 Mbps.

Membresía de CLARA

Por pertenecer a la red CLARA se deben cancelar 12000 dólares cada año. Este valor es cancelado por todos los miembros de CEDIA.

1.3.2.1 Red Nacional CEDIA

Los costos a los que ofrece Telconet la conexión nacional a CEDIA son de 1 dólar por cada 1 Kbps, por lo que, mensualmente CEDIA debe cancelar 10000 dólares a Telconet.

Se consiguió el aumento de 10 Mbps a 20 Mbps por el mismo valor de 10000 dólares y que cada miembro tenga como mínimo 1 Mbps en su última milla para que por lo menos pueda establecer una videoconferencia de calidad sin necesidad de recurrir el aumento provisional por parte de Telconet.

1.3.2 DIRECCIONAMIENTO

Se encuentra autorizada por la LACNIC (*Latin American and Caribbean Internet Addresses Registry*) la asignación de 16 subredes de direcciones IPv4 clase B para la red CEDIA, las cuales serían asignadas de la siguiente manera entre los miembros:

Miembro	***Dirección de Subed***	***Máscara de Subred***	***Número de direcciones***
CEDIA Backbone	190.15.128.0	255.255.255.192	62
INNOCAR	190.15.128.64	255.255.255.192	62
UNEMI	190.15.128.128	255.255.255.192	62
INP	190.15.128.192	255.255.255.192	62
ESPOL	190.15.129.0	255.255.255.0	254
UCSG	190.15.130.0	255.255.255.0	254
NL	190.15.131.0	255.255.255.0	254
UTPL	190.15.132.0	255.255.255.0	254
UTA	190.15.133.0	255.255.255.0	254
ESPOCH	190.15.134.0	255.255.255.0	254
UNACH	190.15.135.0	255.255.255.0	254
UC	190.15.136.0	255.255.255.0	254
PUCE Ibarra	190.15.137.0	255.255.255.128	126
PUCE Santo Domingo	190.15.137.128	255.255.255.128	126
SENACYT	190.15.138.0	255.255.255.128	126
UIE	190.15.138.128	255.255.255.128	126
EPN	190.15.139.0	255.255.255.0	254
ESPE	190.15.140.0	255.255.255.0	254

Miembro	*Dirección de Subed*	*Máscara de Subred*	*Número de direcciones*
UCE	190.15.141.0	255.255.255.0	254
USFQ	190.15.142.0	255.255.255.0	254
UTE	190.15.143.0	255.255.255.0	254

Tabla 1.5 Asignación de Direcciones IPv4 a los miembros de CEDIA

CLARA asignó un bloque de direcciones IPv6 para la red CEDIA, las cuales se distribuyeron de la siguiente manera entre los miembros para realizar pruebas hacia la migración de este protocolo:

Miembro	*Dirección de Red*
CEDIA Backbone	2800:68.:0001::/48
INNOCAR	2800:68.:0002::/48
UNEMI	2800:68.:0003::/48
INP	2800:68.:0004::/48
ESPOL	2800:68.:0005::/48
UCSG	2800:68.:0006::/48
UNL	2800:68.:0007::/48
UTPL	2800:68.:0008::/48
UTA	2800:68.:0009::/48
ESPOCH	2800:68.:000A::/48
UNACH	2800:68.:000B::/48
UC	2800:68.:000C::/48
PUCE Ibarra	2800:68.:000D::/48
PUCE Santo Domingo	2800:68.:000E::/48
SENACYT	2800:68.:000F::/48
UIE	2800:68.:0010::/48
EPN	2800:68.:0011::/48
ESPE	2800:68.:0012::/48
UCE	2800:68.:0013::/48
USFQ	2800:68.:0014::/48

Miembro	*Dirección de Red*
UTE	2800:68.:0015::/48

Tabla 1.6 Asignación de direcciones IPv6 a los miembros de CEDIA

También existe la autorización por parte de LACNIC para la asignación de un bloque de direcciones IPv6 para la red CEDIA.

1.4 COMPARACIÓN ENTRE LAS ESTRUCTURAS DE RED DE CEDIA Y REUNA

REUNA (Red Universitaria Nacional) es la organización chilena que permite en este país el acceso a las redes avanzadas. Chile fue el primer país conectado a la red CLARA, por lo cual, actualmente es un nodo de la troncal.

1.4.1 EVOLUCIÓN

1.4.1.1 Reuna2

En un inicio la red de datos física o troncal fue denominada REUNA2, esta red estuvo aliada a la empresa Telefónica Chile, el mayor impacto de la alianza consistió en el aporte de servicios que permitió establecer una red de banda ancha de 155 Mbps, basada en la red SDH (*Synchronous Digital Hierarchy*) de Telefónica, que con el uso de tecnología ATM (*Asynchronous Transfer Mode*) logró enlazar a todas las instituciones del Consorcio.

1.4.1.2 GReuna

GREUNA es la nueva versión de REUNA2. Esta red de mejores características fue implementada a fines del 2006 con nuevos equipos que permiten soportar la nueva capacidad de 1 Gbps, debido a esto se antepone la “G” a su nombre.

Los nuevos dispositivos de acceso tienen una capacidad de procesamiento 150 veces mayor, mientras los utilizados en REUNA2, enrutadores Cisco 7204, soportaban 100 Kpps (kilo paquetes por segundo) los utilizados en GREUNA, enrutadores Cisco 6503, soportan mínimo 15 Mpps (mega paquetes por segundo).

Los nuevos equipos soportan QoS (Calidad de Servicio), control de tráfico P2P (Peer to Peer), prevención y control de ataques tales como DoS (Negación de Servicio), entre otros.

GREUNA también posee equipos que permiten realizar una mejor administración de la red, equipos que soportan tráfico *Multicast* e IPv6 para algunos segmentos de red.

El cambio de REUNA2 a GREUNA se dio sin ningún inconveniente ya que los miembros de REUNA se enlazan a la troncal a través de fibra.

Este cambio se produjo ante todo para posibilitar a todos los miembros de REUNA, además de tener mayores capacidades, tener mayores seguridades a nivel de aplicaciones, un mayor control del tráfico, una mejor administración de las redes que permita medir el desempeño y así eliminar problemas de saturación, entre otros.

REUNA ha implementado un sistema en el que se garantice sobre todo la calidad de servicio, para lograrlo utiliza un Sistema de Replicación Dinámica de Contenidos (Proxy o Caché) de alta capacidad lo cual le permite atender los requerimientos de los usuarios con menores tiempos de respuesta, de manera que las aplicaciones demandantes de mayor ancho de banda lo tengan disponible, como por ejemplo videoconferencias, entre otros.

1.4.1.3 Reuna Tec

REUNA Tec es la gerencia técnica de REUNA, consiste en un grupo de Ingenieros del área de redes que en forma permanente buscan nuevos servicios o mejoras en los existentes.

1.4.1.4 Conexión a REUNA

GREUNA utiliza tecnología *Gigabit Ethernet* de 1 Gbps y ATM de 155 Mbps, esta red es de uso exclusivo para sus socios. Cada miembro se conecta a través de un enlace de 15 Mbps a la red IP nacional. GREUNA se conecta a la red Internet nacional mediante conexiones directas o por accesos a puntos de intercambio de tráfico local, con esto REUNA logra obtener enlaces de alta velocidad con los proveedores de servicio de Internet.

Características de GREUNA:

- Calidad de servicio
- Multiplexación 1:1
- Monitoreo y control de calidad permanente (las 24 horas los 365 días del año).
- Administración compartida de la red, aplicando políticas de seguridad y control de la conexión.
- Tráfico en tiempo real.
- Disponibilidad de la red del 99.99%.
- Clasificación de tráfico.
- Soporte *Multicast* e IPv6.

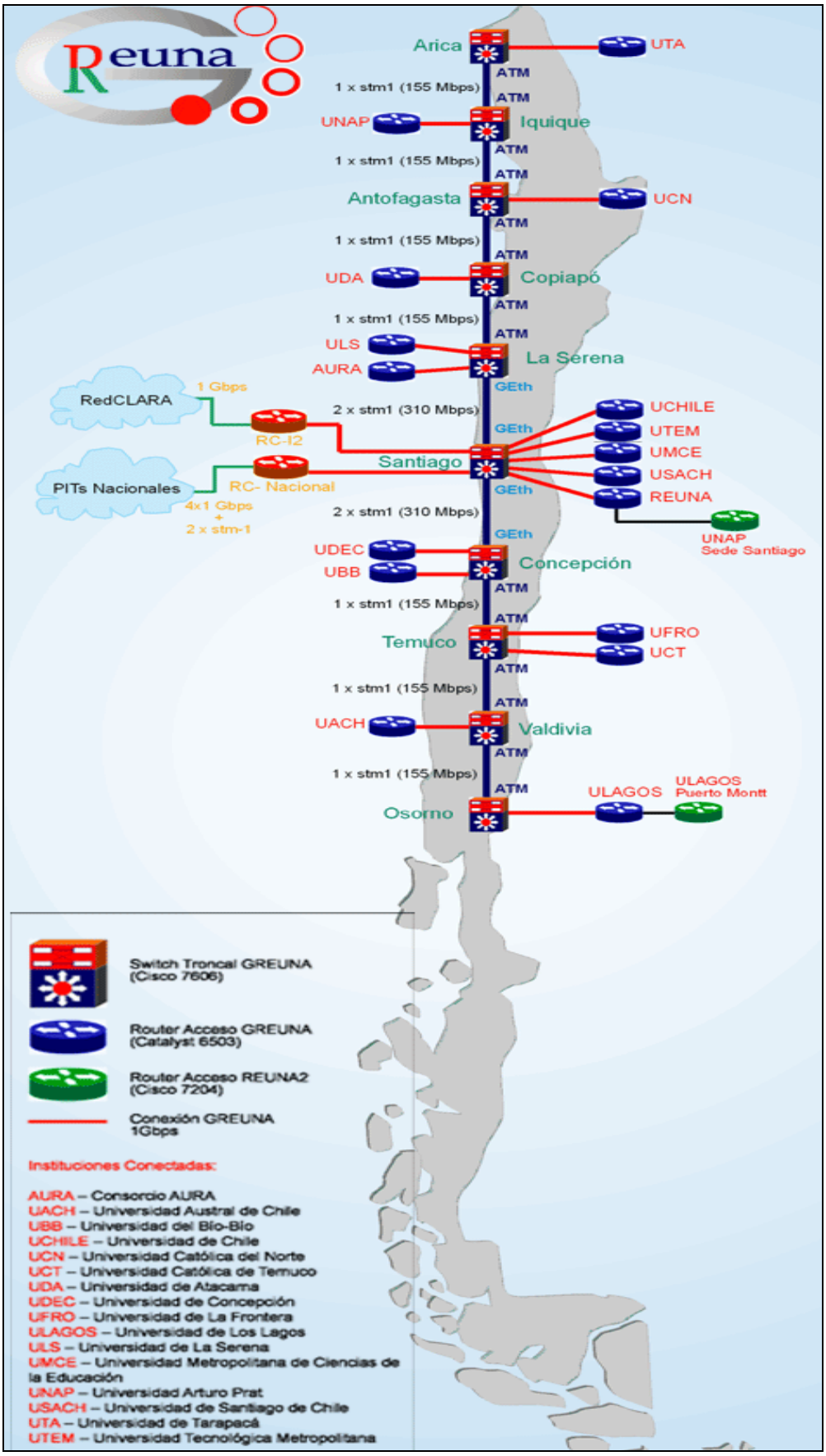


Figura 1.8 Topología de GREUNA [4]

1.4.1.5 Servicios

Entre los principales servicios ofrecidos por REUNA se tienen:

Doctor Red

Este servicio da la posibilidad de conocer el estado de su conexión hacia las redes avanzadas.

Permite:

1. Verificar si existe conexión entre un computador y las redes avanzadas.
2. Verificar si el computador con el que desea enlazarse se encuentra conectado a las redes avanzadas.
3. Analizar las características de conexión entre 2 estaciones o servidores a través de las redes avanzadas.

IPv6 (Protocolo Internet versión 6)

CLARA ha asignado a todos sus miembros un bloque de direcciones IPv6.

REUNA actualmente utiliza IPv6 para conectarse con las redes académicas internacionales a través de CLARA, cuenta con el bloque de direccionamiento 2001:1310::/16 asignado por LACNIC, es decir, direcciones del tipo 2001:1310:abcd::/48 se le asignarán a cada institución miembro, siendo abcd administrados por REUNA, en cuanto a las direcciones 2001:1310:abcd:efgh::/64 serán asignados por cada institución, las cuales administrarán los campos efgh.

VRVS (*Virtual Room Videoconferencing System*)

El Sistema de Sala Virtual de Conferencia está basado, como su nombre lo indica, en salas virtuales en donde los usuarios interactúan mediante 3 elementos:

1. Videoconferencia
2. Pantalla de conversación escrita (chat).
3. Mecanismo para compartir documentos y aplicaciones.

REUNA ofrece gratuitamente este servicio a sus miembros, para acceder a este sistema.

REUNA ofrece distintas tecnologías de videoconferencia a sus usuarios sin que el uso de una u otra afecte la calidad de servicio, entre ellas tenemos: H.323, VIC-RAT, AccesGrid.

1.4.2 COMPARACIÓN CON CEDIA

- CEDIA, en la actualidad, tiene contratados 10 Mbps con CLARA, lo que comparado con los 1 Gbps que tiene contratado REUNA, le hace notar como una red muy inferior en cuanto a capacidad.

- La red CEDIA se encuentra implementada sobre la infraestructura de fibra óptica de la compañía Telconet, de esta manera logra interconectar nacionalmente a la mayoría de sus miembros, REUNA posee una infraestructura de red propia, lo cual le permite ajustarse a los requerimientos para soportar las aplicaciones desarrolladas para las redes avanzadas.

- REUNA ofrece a sus miembros una serie de servicios, los cuales no son ofrecidos por CEDIA en la actualidad, como *multicast* sobre IPv6, Doctor Red.

- Ecuador se encuentra todavía en procesos de pruebas para la migración hacia IPv6.

- CEDIA debido a la falta de infraestructura propia no ofrece servicios adicionales a los ofrecidos por las redes avanzadas, por lo que, existe una gran brecha entre la red de REUNA y la de CEDIA.

1.5 COMPARACIÓN ENTRE LAS ESTRUCTURAS DE RED DE CEDIA Y RNP

RNP (Red Nacional de Enseñanza e Investigación) es la red encargada de la unión de las redes académicas de Brasil a las redes avanzadas del mundo.

RNP posee uno de los nodos de la red CLARA en la ciudad de Sao Paulo, a través de este nodo se une a la red GÉANT2 de Europa a 622 Mbps.

1.5.1 BACKBONE

RNP posee una de las infraestructuras más robustas a nivel de Latinoamérica, posee 27 puntos de presencia (PoPs) en las principales ciudades del país. La velocidad de conexión entre los PoPs llega a 622 Mbps, garantizando con esto el uso de las aplicaciones del Internet actual tales como: navegación, correo electrónico, transferencia de archivos, entre otros; además de las aplicaciones desarrolladas para redes avanzadas.

En la figura 1.9 se muestra el *backbone* de RNP.

1.5.1 TECNOLOGÍAS SOPORTADAS EN LA RNP

Entre las más importantes se tiene:

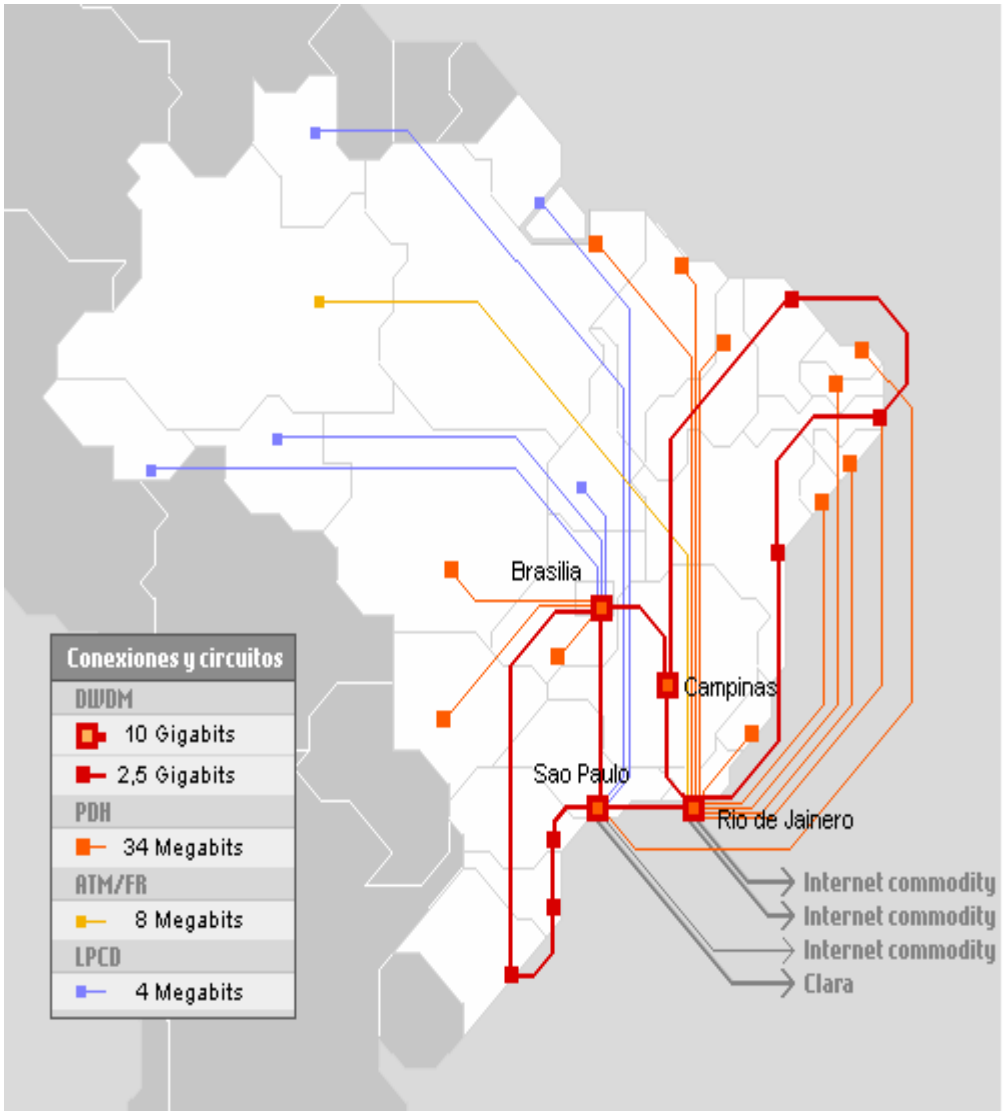


Figura 1.9 *Backbone* de RNP [5]

Multicast

Los *enrutadores* de la RNP son capaces de hacer enrutamiento *multicast*, los utilizados en los PoPs son los Cisco 7507, en los demás se está implementando un túnel DVMRP (*Distante Vector Multicast Routing Protocol*) entre un equipo en el PoP y el enrutador 7507 más cercano del *backbone*, lo que se desea alcanzar con esto es que todos los PoPs soporten *multicast* nativo en sus enrutadores.

NTP

La RNP posee un servidor NTP (*Network Time Protocol*) conectado directamente a un reloj de referencia de altísima precisión.

Para distribuir la carga de procesamiento y garantizar un servicio confiable la RNP posee una jerarquía de servidores NTP.

QoS

Las redes avanzadas se caracterizan por garantizar calidad de servicio a sus aplicaciones, es por esto que la RNP implementó en sus enrutadores servicios diferenciados, dando mayor importancia a las aplicaciones multimedia que corren en tiempo real tales como: videoconferencia y video/audio *streaming*.

IPv6

La RNP configuró una red en la que tanto IPv4 como IPv6 trabajan paralelamente sin que interfieran el uno en el otro.

La RNP es responsable de la distribución de direcciones IPv6 en Brasil. IPv6 ha sido comercialmente más utilizado en el área de la telefonía específicamente en los denominados teléfonos celulares de tercera generación.

Conexiones entre RNP y redes extranjeras

La red IPv6 de la RNP se encuentra conectada con las redes:

- Ampath – *Americas Path Network*(EEUU)
- RCTS – *Rede Ciência, Tecnologia e Sociedade* (Portugal).

Además posee túneles IPv6, los cuales consisten en enlaces virtuales sobre IPv4, con las redes:

- Internet2 (EEUU)
- Renater *Le Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche* (Francia).

Videoconferencia

RNP ofrece el servicio de videoconferencia a la comunidad brasilera de enseñanza e investigación a través de un Sistema de Salas Virtuales de Videoconferencia (VRVS) del Instituto de Tecnología de California (CAITECH).

RNP posee en su *backbone* reflectores, que son computadoras con *software* específico que establecen un túnel IP permanente, usados por los participantes para acceder a las VRVS en Brasil. En la actualidad, el VRVS cuenta con tres reflectores disponibles en Brasil (dos en Río de Janeiro y uno en Río Grande do Sul).

A través de las videoconferencias RNP ha hecho posible la comunicación entre equipos de trabajo como el Servicio de Soporte a Operaciones (SSO), el Centro de Ingeniería y Operaciones (CEO) y el Directorio de Administración.

1.5.2 COMPARACIÓN CON CEDIA

- Al igual que RNP, CEDIA al pertenecer a las redes avanzadas del mundo, estaría en la capacidad de soportar las mismas aplicaciones.

- RNP tiene una capacidad en los enlaces entre sus nodos principales de 622 Mbps, esto es 300 veces superior a la conexión existente en el Ecuador.

- CEDIA no tiene conexión directa con redes avanzadas como Internet2, logra enlazarse a éstas, a través de la conexión existente con el nodo de Chile.

- CEDIA no posee una infraestructura de red propia, la cual pueda administrar y configurar de acuerdo a las necesidades de los miembros y del avance tecnológico.

Se puede llegar a la conclusión, luego del análisis comparativo entre las redes mejor estructuradas y organizadas a nivel de Latinoamérica, que en el Ecuador falta difusión de las ventajas que se tiene al alcance, para de esta manera aprovecharlas y proyectarse a proveer de mayores beneficios a la sociedad.

1.6 ANÁLISIS FODA DE CEDIA

Mediante este proceso se analizarán las Fortalezas, Oportunidades, Debilidades y Amenazas de CEDIA. Se considerarán todos los factores que influyan en el desempeño de la institución a nivel interno y externo, y con ello en el cumplimiento de la misión de la misma.

En el ámbito interno se analizarán las Fortalezas y Debilidades y en el externo se analizarán las Oportunidades y las Amenazas.

1.6.1 FORTALEZAS

F.1 CEDIA es una institución de prestigio a nivel nacional.

F.2 CEDIA es una organización ligada a las tecnologías de la información y comunicación, las cuales lideran en la actualidad debido a la importancia de mantener una sociedad informada y comunicada.

F.3 CEDIA a través de las redes avanzadas facilitan el acceso y difusión de la información.

F.4 CEDIA facilita la comunicación e ínter-operación a nivel mundial, debido que a través de ella se tiene acceso a las demás redes avanzadas del mundo.

F.5 CEDIA, al ser una red privada, provee de mayor seguridad al usuario.

F.6 CEDIA ofrece una red avanzada dedicada para investigadores y estudiantes.

F.7 CEDIA permite concentrar recursos humanos y técnicos a pesar de no compartir el mismo campus.

F.8 9 Universidades entre las mejores a nivel del Pacto Andino.

F.9 CEDIA posee un directorio conformado por representantes de todos los miembros, los cuales periódicamente se reunen para plantear ideas en mejora de la institución.

F.10 CEDIA permite interconectar las universidades para propósitos educativos y de investigación a través de una red privada.

1.6.2 DEBILIDADES

D.1 Insuficientes recursos económicos.

D.2 Falta de estimulación del uso de la red avanzada.

D.3 Falta de difusión de las ventajas que nos provee el ser miembro de una red avanzada.

D.4 Falta de aplicaciones colaborativas entre los miembros debido al poco uso de la red avanzada.

D.5 Poca demanda de conectividad.

D.6 Falta de preparación en cuanto a formación académica transnacional.

D.7 Falta de infraestructura humana dedicada a la red avanzada.

D.8 Falta de una red dedicada propia.

D.9 Falta de establecimientos de comunidades virtuales.

D.10 Falta de participación en proyectos de investigación internacionales.

D.11 Falta de interés por parte de los representantes en difundir el acceso.

1.6.3 OPORTUNIDADES

O.1 CEDIA es la única organización autorizada en Ecuador de permitir el acceso de sus miembros a las redes avanzadas.

O.2 Incremento del acceso a la red en instituciones educativas y de Investigación.

O.3 Apoyo de entidades internacionales.

O.4 Redes de colaboración humana y tecnológica mundiales.

O.5 Acceso remoto a recursos científicos.

O.6 Interés por parte de las instituciones educativas en poseer una red exclusiva para formación académica e investigación.

O.7 Acceso a nuevas tecnologías.

O.8 Gran cantidad de servicios por ofrecer.

1.6.4 AMENAZAS

A.1 Red Avanzada Internet 2 permitirá el acceso público.

A.2 Recursos provistos por CLARA.

A.3 Enorme brecha entre los países desarrollados y los subdesarrollados en cuanto a manejo de tecnología.

A.4 Falta de apoyo gubernamental.

A.5 Término del proyecto ALICE en Marzo del 2008.

A.6 Alza de costos de conexión internacional.

A.7 Inestabilidad política.

A.8 Inestabilidad macroeconómica.

A.9 Dependencia de un proveedor de servicios privado.

A.10 Escasos servicios ofrecidos en comparación a otras redes a nivel de Latinoamérica.

1.6.5 ESTRATEGIAS (FORTALEZAS Y OPORTUNIDADES)

E1. Mantener y mejorar en lo posible las condiciones de acceso y uso de la red avanzada de modo que exista siempre disponibilidad y calidad de servicio garantizado

E2. Fortalecer la presencia de la institución a nivel de Latinoamérica de modo que sea de gran prestigio a nivel internacional y de esta manera motivar a las instituciones académicas y de investigación a pertenecer a CEDIA

E3. Gestionar el desarrollo y cumplimiento de los proyectos planteados, de modo que contribuyan al mejoramiento de CEDIA

E4. Proponer nuevos programas de investigación y desarrollar nuevas aplicaciones que colaboren con el desarrollo científico del país.

1.6.6 ESTRATEGIAS (FORTALEZAS Y AMENAZAS)

E1. Difundir el conocimiento de las TICs a través de programas de instrucción tecnológica al alcance de todos los usuarios.

E2. Planteamiento de soluciones de interconexión entre los miembros de acuerdo a la realidad del país, de modo que exista la menor incapacidad posible de acceso a la red avanzada.

E3. Optimizar el uso de recursos de modo que se permita ofrecer mayor cantidad de servicios sin tener que invertir más.

E4. Reducir desigualdades entre la red avanzada ecuatoriana y las demás a nivel de Latinoamérica.

E5. Realizar convenios con el Estado o con entidades privadas, para obtener financiamiento para las operaciones de CEDIA.

1.6.7 ESTRATEGIAS (DEBILIDADES Y OPORTUNIDADES)

E1. Incrementar la oferta de membresías para nuevas instituciones académicas interesadas en acceder a una red dedicada a la educación e investigación.

E2. Impulsar que un mayor número de personas participe en los proyectos que se realizan a nivel mundial a través de las redes avanzadas.

E3. Proponer iniciativas que nos lleven a mantener el apoyo internacional.

E4. Analizar las características de los miembros en cuanto a necesidades de recursos tecnológicos y diseñar planes de incentivo a la conexión.

E5. Orientar a los representantes de cada institución miembro a la difusión de las ventajas que se tienen a disposición al pertenecer a una red avanzada.

1.6.8 ESTRATEGIAS (DEBILIDADES Y AMENAZAS)

E1. Impulsar la colaboración, tanto de miembros académicos como estratégicos, con los recursos necesarios para ofrecer un servicio seguro y garantizado.

E2. Incentivar al uso de los recursos de la red avanzada y aprovechar las ventajas brindadas por la misma, para con ello intervenir en la productividad y desarrollo con la utilización de todo lo que tienen disponible al pertenecer a CEDIA.

E3. Incrementar la participación de los miembros en los proyectos que aporten al crecimiento y fortalecimiento de la institución.

E4. Fortalecer programas que permitan la vinculación de nuevos miembros a la red avanzada ecuatoriana.

1.6.9 MATRIZ FODA

FODA		DEBILIDADES											FORTALEZAS									
		D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10
AMENAZAS	A1		E2	E2		E2						E2		E1								
	A2	E1																			E5	
	A3		E2	E2		E2						E2						E1				E4
	A4	E1																	E2		E2	
	A5	E1																			E5	
	A6	E1		E4																		E4
	A7			E4																	E5	
	A8			E4																		
	A9																				E2	
	A10				E3		E3			E3		E3							E3		E3	
OPORTUNIDADES	O1			E5								E5			E1			E1			E1	
	O2					E4				E2					E1							
	O3	E3																E4				
	O4						E2				E2					E4						
	O5																		E4			
	O6			E1																E2	E3	
	O7													E3								
	O8		E4										E2									E3

Tabla 1.7 Matriz FODA

1.6.10 MATRIZ DE EVALUACIÓN DE FACTORES INTERNOS (MEFI)

Factores críticos para el éxito	Peso	Calificación	Total Ponderado
FORTALEZAS			
F1	0.025	3	0.075
F2	0.05	3	0.15
F3	0.05	3	0.15
F4	0.05	4	0.2
F5	0.025	3	0.075
F6	0.075	4	0.3
F7	0.05	4	0.2
F8	0.025	3	0.075
F9	0.075	4	0.3
F10	0.075	4	0.3
DEBILIDADES			
D1	0.075	1	0.075
D2	0.05	1	0.05
D3	0.05	1	0.05
D4	0.025	2	0.05

D5	0.025	2	0.05
D6	0.05	1	0.05
D7	0.05	1	0.05
D8	0.075	1	0.075
D9	0.025	2	0.05
D10	0.025	2	0.05
D11	0.05	1	0.05
		TOTAL	**2.425**

Tabla 1.8 Matriz MEFI

De los resultados obtenidos en la matríz MEFI, se puede concluir, que la institución es débil internamente, pero no está lejos de fortalecerse siempre y cuando se cumpla con un plan estratégico que permita superar las debilidades.

2 ANÁLISIS DE LAS APLICACIONES DE LAS REDES AVANZADAS

2.1 ANÁLISIS DE LAS PRINCIPALES APLICACIONES EXISTENTES PARA LAS REDES AVANZADAS

2.1.1 BIBLIOTECAS DIGITALES [7]

2.1.1.1 Definición

Las bibliotecas digitales son sistemas complejos y avanzados que involucran el manejo de información de muy diversa naturaleza, además de la preservación digital de documentos, filtrado y recuperación de información, manejo de derechos intelectuales de autor, servicios de información multimedia, entre otros. Se basan en el principio de que todos los usuarios tienen las mismas posibilidades de acceso a los recursos de la biblioteca, independientemente del lugar geográfico en el que se encuentren.

De acuerdo con esta definición la biblioteca digital es más que un conjunto de recursos de información, pues es un servicio que se basa en principios de selección, adquisición, acceso, administración, protección y preservación de la información que se brinda a un usuario específico.

Una biblioteca digital mantiene un servicio permanente, multiusuario, que posibilita acceder a los servicios tradicionales de una biblioteca presencial y una serie de servicios adicionales integrados en el diseño de la biblioteca digital, como por ejemplo la posibilidad de incorporar técnicas de recuperación de textos para permitir búsquedas de documentos por su contenido o temática.

2.1.1.2 Contenido

La biblioteca digital almacena:

- Datos estructurados, no estructurados.
- Textos transcritos.
- Textos etiquetados en HTML (*HyperText Markup Language*), XML (*e**X**tensible **M**arkup **L**anguage*), SGML (*Standard Generalized Markup Language*), entre otros.
- Imágenes.
- Video.
- Audio.
- Catálogos automatizados.
- Resúmenes.

Los catálogos automatizados brindan mejoras en los servicios, permitiendo el acceso remoto, la consulta concurrente de los registros, además del beneficio que nos brindan las referencias hiper-textuales lo cual nos proporciona una mayor calidad de los servicios online.

La información que se puede encontrar en las bibliotecas digitales que existen actualmente cubren áreas como: finanzas, mercadotecnia, literatura, ingenierías, educación, computación, medicina, música, entre otras. Como gran parte de la información almacenada en la biblioteca digital son datos no estructurados[1], éstas mantienen sistemas capaces de aplicar técnicas de recuperación de textos. Estos

[1] Las colecciones no estructuradas son datos sin tipos pre-definidos, se almacenan como documentos u objetos sin estructura uniforme.

Ejm. Correspondencia, diarios, novelas, blogs.

sistemas implementan métodos que permiten a un usuario realizar búsquedas por contenido, de forma que sea posible localizar aquellos documentos, datos, páginas digitalizadas, imágenes, videos, audio, entre otros, relevantes en función de los términos de búsqueda que se hayan indicado, es decir, dada una consulta, obtener todos los documentos relevantes posibles y minimizar el número de documentos irrelevantes.

Para poder llevar estadísticas de la información que es consultada se pueden incluir contadores, de esta manera, se evalúan las consultas a bases de datos o a sitios de interés a los que se haga referencia.

2.1.1.3 Estructura de una Biblioteca Digital

La estructura de la biblioteca digital se basa en el tipo de interacción del servicio entre usuarios y bibliotecarios, así se tiene:

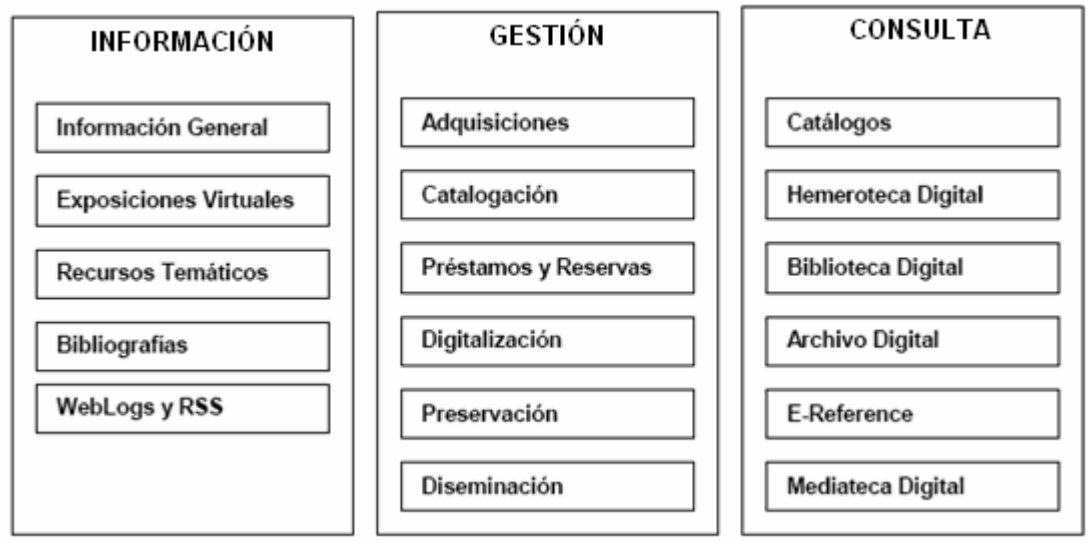


Figura 2.1 Estructura de la Biblioteca Digital [7] [2]

[2] Un RSS es un archivo generado por algunos sitios web (y por muchos weblogs) que contiene una versión específica de la información publicada en esa web.

Área de Información: Se encontrarán todos aquellos servicios donde existen datos no estructurados, como puede ser la publicación de información general sobre el funcionamiento de la institución, políticas y normas.

Área de Gestión: En el área de gestión aparecerán todos aquellos servicios asociados al funcionamiento a través de los sistemas integrales de gestión de bibliotecas.

Área de Consulta: Es una de las áreas temáticas más importantes por su propia naturaleza en el acceso a la información.

2.1.1.4 Requisitos de Usuario

Una biblioteca digital ha de permitir que los usuarios puedan realizar conexiones remotas siguiendo una arquitectura cliente/servidor. Se debe considerar que los usuarios que deseen acceder a los servicios de la biblioteca digital no necesitan de un amplio conocimiento acerca del funcionamiento de la misma, por consiguiente se necesita de una interfaz amigable, intuitiva, fácil de utilizar para obtener el mayor rendimiento esperado.

2.1.1.5 Ventajas

La información que se puede encontrar en las bibliotecas digitales, en algunos casos se puede imprimir, grabar, mandar por correo electrónico e incluso manipular. Estas características las convierten en un gran recurso para científicos, profesores y alumnos principalmente.

Las Bibliotecas Digitales permiten:

- Ahorro de papel.
- Crecimiento y mejor organización de la información.
- Optimización de los mecanismos de búsqueda de textos, imágenes, videos y audio.
- Facultad de acceder a información desde cualquier parte del mundo e igualmente compartirla.

2.1.1.6 Desventajas

Al poder tener la información en formato digital y ser tan sencilla su distribución, se deriva una desventaja, los derechos y beneficios que corresponden a los autores de las obras se ven amenazados. Se requiere entonces protección de los derechos de los autores y de los lectores para que estos últimos puedan seguir teniendo acceso a información confiable.

Para limitar el duplicado indebido de la información los sitios toman medidas como:

- Se implementan páginas que no permiten la copia o impresión de las páginas de los sitios y así el usuario sólo tiene permisos de lectura.

- Discos compactos que incluyen llaves que no permiten la copia de la información a disco duro, o tienen integrada una clave de registro que autoriza instalar una sola vez el producto.

2.1.1.7 Proyectos Sociales de las Bibliotecas Digitales

Entre los proyectos que se están realizando para enriquecer las bibliotecas digitales, se encuentran los *talking books* que salieron al mercado para las

personas que padecen de la vista y que no tienen la posibilidad de aprender el sistema Braille.

Para los *talking books* se está digitalizando el audio y se incorpora en las bibliotecas digitales; en aquellas que no lo son, se tienen en disco compacto o *cassette* y se tienen a disposición del público con el equipo necesario para poder ser escuchados.

2.1.2 TELE-INMERSIÓN [8]

2.1.2.1 Definición

Es una combinación de sistemas avanzados de telecomunicaciones que permite a usuarios en sitios geográficamente distribuidos colaborar en tiempo real en un ambiente compartido, simulado, híbrido como si estuvieran en la misma habitación.

Los usuarios pueden compartir y manipular datos, compartir experiencias, simulaciones, etc. La tele-inmersión es un nuevo sistema de interacción humana a través de técnicas digitales que proporciona al usuario la ilusión de compartir un mismo espacio físico con otras personas, aunque se hallen alejadas grandes distancias.

Para ello utilizan los procesos de visualización con nuevas técnicas de visión que trascienden las tradicionales limitaciones de una cámara. En vez de ceñirse a observar personas y su entorno inmediato desde una sola posición, las estaciones de tele-inmersión las reproducen como "esculturas animadas", sin limitarse a favorecer una perspectiva exclusiva. El resultado es que todos los participantes, por alejados que estén, pueden compartir y explorar un espacio de proporciones naturales. [9]

2.1.2.2 Estructura del Sistema Tele-Inmersivo

En un ambiente tele-inmersivo los sensores y cámaras reconocen la presencia y los movimientos de individuos y de objetos, capturando esos individuos y objetos mediante imágenes que serán proyectadas posteriormente en múltiples entornos geográficamente distribuidos. Esto requiere tener que realizar un muestreo del ambiente físico, así como de las caras y los cuerpos de los usuarios.

El proceso de la captura del entorno hasta la presentación estereoscópica atraviesa las siguientes fases:

2.1.2.2.1 Seguimiento y Adquisición

El proceso comienza con un conjunto de cámaras y sensores que realiza un seguimiento del usuario y su entorno. El escenario es capturado desde diferentes ángulos mediante las cámaras, donde cada dispositivo genera varias imágenes por segundo desde su correspondiente punto de vista. Figura 2.2. Las cámaras son agrupadas en parejas o tríos y se realiza su elección dependiendo de la posición relativa del interlocutor remoto.

2.1.2.2.2 Simplificación y modelado en 3D

Para cada trío de imágenes seleccionadas se crea un mapa de disparidad, reflejando el grado de variación entre las imágenes en todos los puntos del campo visual. Las desigualdades son analizadas para resolver las diferencias entre las imágenes de las tres cámaras.

Los valores resultantes son combinados en mapas de profundidad de la escena. Todos los mapas, a su vez son mezclados para obtener un modelo de un punto de vista independiente en un instante concreto. El proceso combinatorio de los mapas proporciona la posibilidad de eliminar ruido y puntos esporádicos.

El modelado de la escena objetivo consigue una sensación de realidad superior a las imágenes de video planas, esto se consigue mediante imágenes a tamaño real estereoscópicas en 3D.

2.1.2.2.3 Compresión y Transmisión

Con la captura y el cálculo del modelo 3D resultante, el siguiente paso consiste en comprimir los datos mediante diferentes técnicas y enviarlos por redes de alta velocidad.

2.1.2.2.4 Descompresión y Reconstrucción

El modelo recibido es descomprimido y reconstruido, a partir de la reconstrucción se generan dos imágenes estereoscópicas.

2.1.2.2.5 Representación

En esta fase es en donde finalmente las dos imágenes estereoscópicas de la escena son proyectadas en el *display* teniendo en cuenta la posición de usuario y la calibración de los proyectores. Figura 2.3

2.1.2.3 Requerimientos del Sistema

La tele-inmersión requiere de una gran infraestructura de red, que contenga características como:

- **Gran ancho de banda**, cuyo valor se encuentra en el orden de decenas de Megabits por segundo.

- **Bajo retardo**, cuyo valor se encuentra en el orden de cientos de milisegundos hasta uno o dos segundos.

- **Bajo jitter**, este valor está alrededor de las decenas de milisegundos.

- Tecnologías avanzadas como *Multicast*.

Figura 2.2 Semicírculo de cámaras [10]

2.1.2.4 Ventajas

- Con la utilización de la tele-inmersión se pueden realizar múltiples actividades, ya sea en el campo educativo, de negocios, cultural entre otros.

- Se puede realizar videoconferencia en 3D, evitando que los participantes dejen su lugar de trabajo o vivienda.

Figura 2.3 Sala de Conferencias con Tele-inmersión [11]

2.1.2.5 Proyecciones al futuro

El futuro de la tele-inmersión depende de muchos factores, aunque hasta el momento ya se ha logrado crear ambientes de tele-conferencias en 3D, la tendencia apunta a que los participantes no solo se puedan ver, sino también sentir, ya sea entre ellos, o compartir objetos a los cuales los puedan tocar, sentir, oler, todo esto dependerá del avance de muchos elementos electrónicos que permitan que los participantes realicen estas actividades.

2.1.3 LABORATORIOS VIRTUALES

2.1.3.1 Definición

Un laboratorio virtual se define como “simulaciones de prácticas manipulativas que pueden ser hechas por la/el estudiante lejos de la universidad y el docente”. [12]

El laboratorio virtual es un conjunto de equipos (Instrumentos de medida, equipos informáticos, programas) ubicados en uno o varios lugares, que se ofrece a los usuarios, situados en cualquier lugar, para que puedan trabajar con ellos.

Es una infraestructura de pruebas que no existe físicamente en el sitio en que se encuentran los realizadores de esos experimentos, pero puede existir en otro lugar del planeta o haber sido creado electrónicamente dentro de un sistema computacional.

Como cualquier otro laboratorio, las herramientas y las técnicas son específicas al dominio de la investigación, pero los requisitos básicos de la infraestructura se comparten a través de disciplinas. Aunque está relacionado con algunas de las aplicaciones de la tele-inmersión, el laboratorio virtual no asume a priori la necesidad de un ambiente de tele-presencia compartido.

2.1.3.2 Tipos de laboratorios virtuales [13]

Existen dos enfoques bajo los que se desarrolla la tecnología de los laboratorios virtuales:

- Laboratorios virtuales por simulación.
- Laboratorios virtuales por acceso remoto.

En el primer caso, se utiliza *software* y *hardware* que permite la posibilidad de modelar experimentos y experiencias (simulación), con interactividad gráfica apropiada.

En el segundo caso, se debe subdividir de acuerdo a las prestaciones que brinde el laboratorio, que podría ir desde la utilización de un *software* básico hasta el

manejo de equipos y dispositivos reales ubicados en sitios diferentes a aquellos en que se encuentran quienes realizan los experimentos (acceso remoto).

2.1.3.3 Elementos del laboratorio virtual [13]

El laboratorio virtual es una extensión o complemento a los laboratorios reales, abriendo nuevas oportunidades que probablemente no sean viables de implementar económica y socialmente a través de un laboratorio real.

La infraestructura tecnológica de los laboratorios virtuales generalmente tiene algunos o todos los componentes siguientes:

- Servidores de computación capaces de manejar reducciones de datos y simulaciones a gran escala.

- Bases de datos que contengan información específica para aplicaciones, tales como simulación inicial y condiciones límite, observaciones experimentales, requerimientos de clientes, restricciones de fabricación.

- Instrumentos científicos conectados a la red.

- Herramientas de colaboración, que a veces incluyen la tele-inmersión.

- *Software* especializado para simulación, análisis de datos, descubrimiento, reducción y visualización.

2.1.3.4 Esquema general de la estructura de un laboratorio [14]

2.1.3.4.1 Cliente

El usuario de un laboratorio virtual.

2.1.3.4.2 Servidor de Laboratorio

Constará principalmente de un servidor *web*. El laboratorio debe disponer de un sistema eficaz de gestión de los recursos de que dispone. Para ello, un computador se deberá encargar de conocer qué sistemas de medida hay disponibles y qué configuración de medida tiene cada uno. Por otra parte, cada montaje tendrá unos posibles usuarios, a los que se les permitirá el acceso siguiendo una determinada política:

- Nombres,
- Horas de acceso,
- Experiencias permitidas.

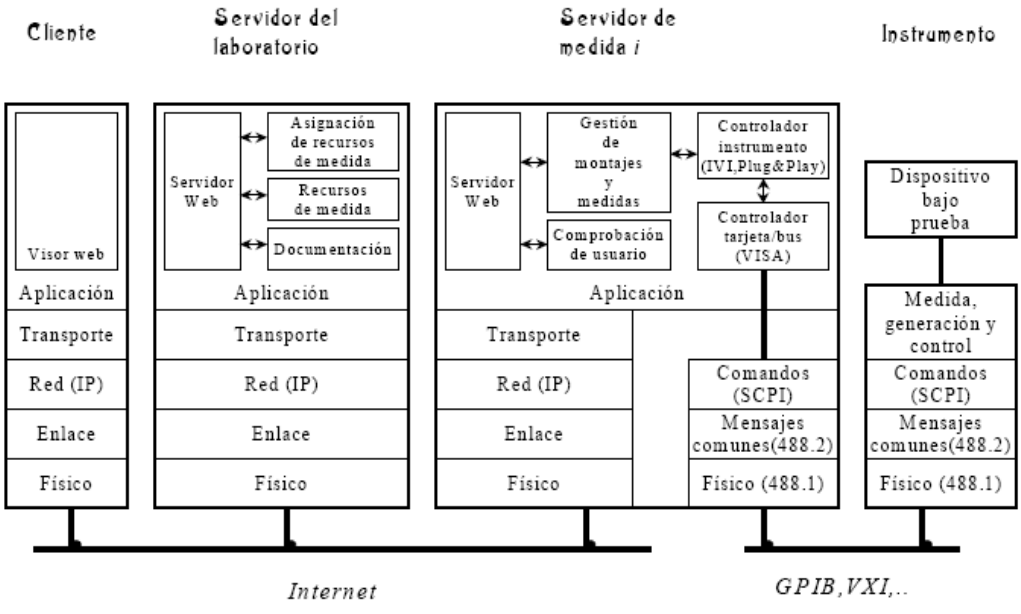


Figura 2.4 Esquema general de un laboratorio virtual [14]

Finalmente, habrá una serie de documentación asociada al laboratorio que necesitará ser consultada antes de trabajar con los equipos (Manuales de los instrumentos, descripción de montajes, reglas de funcionamiento del laboratorio). Habrá un servidor de laboratorio por laboratorio.

2.1.3.4.3 Servidor de Medidas

Cada sistema formado por instrumentos y dispositivos bajo prueba está controlado por un computador que se denomina servidor de medidas, pues podrá haber varios en distintos lugares.

Este servidor tiene la información de los instrumentos a los que está conectado y del tipo de medidas que puede hacerse con él. Esta información será la que transmita al servidor del laboratorio para poder ofrecer sus servicios a los usuarios.

El servidor del laboratorio, una vez comprobada y autorizada la petición de servicio por parte de un usuario, transferirá al servidor de medida la identificación del usuario para que sea éste quien controle de ahora en adelante las peticiones de dicho usuario. De esta forma se descarga al servidor del laboratorio de la tarea de hacer de intermediario entre usuarios y medidas, siendo el usuario quien habla directamente con el servidor de medida correspondiente.

El servidor de medida proporcionará al usuario un interfaz gráfica en el que se verán los experimentos a realizar y los mandos de los instrumentos que podrán ser variados para realizar las distintas medidas. Por supuesto, deberá ofrecer en diversa forma los resultados de la medida, bien gráfica o numérica, con la posibilidad de almacenar los datos en un formato adecuado para utilizarlos en un procesado posterior.

A partir de aquí ya entra la parte específica de instrumentación. Actualmente hay organizaciones y consorcios cuyo objetivo es definir las normas a cumplir por instrumentos y sus controladores (programas que permiten el control de las funciones de los instrumentos desde un determinado entorno de programación) para garantizar la máxima ínter-cambiabilidad posible, tanto de equipos como de programas.

SCPI (*Standard Commands for Programmable Instruments)*, IVI (*Interchangeable Virtual Instruments*), VISA (*Virtual Instrument Software Architecture*) y *Plug&Play* son estándares que convendrían seguir para asegurar la compatibilidad.

2.1.3.4.4 Instrumento

El instrumento deberá cumplir las recomendaciones mencionadas anteriormente y disponer de controladores normalizados para permitir su fácil configuración y manejo. La conexión con bus GPIB (*General Purpose Interface Bus*) es la más habitual aunque también son posibles otras como VXI (*VME eXtensions for Instrumentation*), PXI (*PCI eXtensions for Instrumentation*), RS-232 (*Recommended Standard 232*), etc.

2.1.3.5 Niveles de servicio de un laboratorio virtual [14]

Existen varios tipos de laboratorios virtuales, que se enmarcan dentro de niveles de acuerdo a las prestaciones o complejidad de los laboratorios.

- El nivel más sencillo es el que tiene básicamente un texto y dibujos sin movimiento.

- En un segundo nivel de complejidad, existen laboratorios que usan animaciones usando el formato GIF (*Graphics Interchange Format*), compatible con Internet.

- El tercer nivel corresponde a los laboratorios que usan videos para mostrar prácticas verdaderas.

- En el cuarto nivel de complejidad están aquellos laboratorios en los cuales se ve en pantalla objetos o escenas que pueden ser manipulados por un estudiante.

- En el quinto nivel se tienen laboratorios en que la falta de certeza en las mediciones y la variabilidad aleatoria de algunos parámetros limitan el control que tiene el usuario. Para explicar esto se puede usar un símil: en las simulaciones actuales, se puede lanzar una canica digital a un frasco y si se apunta en la dirección correcta, cae dentro. En las futuras simulaciones, factores como el viento y la oscuridad en la habitación digital afectarán la trayectoria, será más difícil acertar. Estos laboratorios imitan, por ejemplo, la falibilidad de la puntería humana.

- El sexto nivel, con máquinas que permiten al usuario mirar una imagen y percibir en su piel las sensaciones correspondientes aunque tiene muy poco control sobre la secuencia de eventos.

- El séptimo nivel corresponde a la nueva tecnología que permite una interacción con otra persona conectada a la red, usando casco y traje.

- El octavo nivel se relacionaría con reproducir experiencias mediante implantes eléctricos dentro del cuerpo humano.

2.1.3.6 Ventajas

- La posibilidad de repetir cuantas veces se requiera un experimento.

- La posibilidad de desarrollar habilidades cognitivas e investigativas a partir del aprendizaje por descubrimiento.

- La capacidad de interacción, simulación y retroalimentación.

- La posibilidad de desarrollar el aprendizaje cooperativo y solidario entre los alumnos.

- El estudiante no tiene que trasladarse al centro universitario para la realización de los laboratorios.

- El laboratorio se podrá realizar en el momento que más le convenga al estudiante.

- El laboratorio muestra gráficas que en la realidad solo las conocería en forma teórica.

- No tiene límite de tiempo para realizar su laboratorio.

- La posibilidad de experimentar teóricamente cambiando condiciones de reacción entre las diferentes sustancias que el sistema nos permite, sin peligro de explosiones, contaminación y gasto económico de materiales.

- La participación activa de los estudiantes, la posibilidad de establecer hipótesis ante una situación simulada.

2.1.4 TELEMEDICINA [15]

2.1.4.1 Definición

Telemedicina significa medicina practicada a distancia, es una herramienta tecnológica para el intercambio de imágenes, voz, datos y video, por algún medio electrónico que permite diagnóstico, opinión de casos clínicos y tratamiento, como también la educación médica. Es el uso de las tecnologías de la información y de las comunicaciones como un medio para proveer servicios médicos ahorrando tiempo y dinero, facilitando el acceso a zonas distantes para tener atención de especialistas.

La telemedicina permite que un médico, o equipo médico, cuide a distancia la salud de un individuo o de un grupo de individuos, mediante el empleo de medios diagnósticos y terapéuticos manejados remotamente.

Otra de las utilidades que presta el uso de la transmisión de datos médicos sobre redes adecuadas, es la educación, donde los alumnos de medicina y enfermería pueden aprender remotamente, apoyados por su profesor y con la presencia del paciente.

2.1.4.2 Campos y servicios de telemedicina

Así podemos definir los siguientes servicios, que la telemedicina presta:

- Servicios complementarios e instantáneos a la atención de un especialista (obtención de una segunda opinión).

- Diagnósticos inmediatos por parte de un médico especialista en un área determinada.

- Educación remota de alumnos de las escuelas de enfermería y medicina.

- Servicios de archivo digital de exámenes radiológicos, ecografías y otros.

Todo esto se traduce en una disminución de tiempos entre la toma de exámenes y la obtención de resultados, o entre la atención y el diagnóstico certero del especialista, el cual no debe viajar o el paciente no tiene que ir a examinarse, reduciendo costos de tiempo y dinero.

En la actualidad, dentro del campo de la telemedicina, ésta se usa básicamente en dos áreas de trabajo: La práctica y la educación.

2.1.4.2.1 PRÁCTICA

Dentro de la práctica es posible resaltar las siguientes formas:

- Telediagnósis.
- Teleconsulta.
- Reuniones médicas para obtener segundas opiniones (Teleconferencia).
- Almacenamiento digital de datos o fichas médicas.

Telediagnósis: Diagnóstico a distancia o diagnóstico remoto, es la técnica que mayor impacto causa, dadas las múltiples ventajas que presenta y el amplio aprovechamiento de la tecnología. Consiste en evaluar o asistir en la evaluación médica de un paciente desde un centro hospitalario que se encuentre distante, haciendo uso de las telecomunicaciones para llevar a cabo esta acción.

Teleconsulta: Es una aplicación que permite apoyar a un médico a distancia para confirmar u obtener por un especialista un diagnóstico clínico confiable.

Teleconferencia: Por medio de videoconferencia, es factible convocar una reunión de especialistas que estén en diferentes locaciones (sin límites geográficos), a fin de debatir diferentes situaciones.

Almacenamiento digital (Ficha electrónica): Consiste en la implementación del respaldo digital de documentos tales como fichas médicas, placas radiológicas o exámenes, de manera de agilizar procesos internos y disminuir el espacio físico de almacenamiento de los mismos. Además esto abre posibilidades de obtención de diagnósticos que no sea en tiempo real por medio de correo electrónico o la publicación de resultados de exámenes vía web para ser consultados por los pacientes.

2.1.4.2.2 EDUCACIÓN

Dentro del área educativa tenemos:

- Clases a distancia desde centros médicos (*e-learning* por medio de videoconferencia).

Clases a distancia (E-*learning*): Es el uso académico de la videoconferencia médica, usando la misma tecnología, un docente puede impartir clases a un grupo o varios grupos de estudiantes que se encuentren distantes.

Básicamente, la educación médica hace uso de las técnicas de videoconferencia, ya que de esta manera se saca mayor provecho a los recursos educativos y las experiencias presentadas en la exposición.

2.1.4.3 Funcionamiento del sistema

Un sistema de telemedicina opera básicamente de la siguiente manera: Existe un centro hospitalario menor que presenta una carencia de profesionales en un(as) área(s) específica(s), dicho centro será asistido por uno de mayor envergadura, el cual dispondrá de los especialistas y el tiempo necesario para la atención de los pacientes de manera “remota”, quienes se encontrarán físicamente en la ciudad donde esté el centro de menor tamaño. Esto conlleva beneficios de ahorro de tiempo y dinero para los pacientes y mejora la gestión de los centros de salud más apartados.

En lo referente a la telemedicina en sus formas de teleconferencia (conferencias médicas a distancia) y educación a distancia, el sistema debe ser similar al de telediagnosis, siendo imperativo la capacidad de montar una videoconferencia.

Si nos referimos a la telemedicina como medio de almacenamiento digital, ésta se presenta como una manera de apoyar la labor de los médicos en la obtención de información de modo rápido y eficiente, permitiendo la manipulación de la misma, para poder llevar registros actualizados y requerir, de ser necesario, una segunda opinión en una forma más fácil y expedita. Además el mantener fichas o registros digitales, conlleva la capacidad de manejar volúmenes de información mayores en menor espacio físico, permite la agilización de procesos internos, lo que entrega como resultado una mejora en la gestión del servicio.

Algunos ejemplos de aplicaciones clínicas ensayadas con éxito incluyen, Teleradiología, Telecardiología, Teledermatología, Telepsiquiatría, etc. Se están empleando servicios de telemedicina en diversos sistemas sanitarios y en una variedad de escenarios, tales como zonas rurales, áreas urbanas, áreas sanitarias, prisiones, cuidados a domicilio, emergencias, conflictos bélicos, entre otros.

2.1.4.4 Requerimientos del sistema

Para que un sistema de estas características funcione bien, se debe contar con los siguientes elementos:

- Equipos capaces de comunicarse (preferiblemente videoconferencia).
- Medio de comunicación (Internet, etc.).
- El hospital o clínica de apoyo que debe gestionar los recursos necesarios (infraestructura, tiempo y principalmente especialistas) para prestar los servicios médicos.

2.1.4.5 Ventajas

- Incremento en la eficiencia de los servicios.
- Incremento en la calidad de los servicios.
- Agilización de los resultados.
- Ahorro de tiempo.
- Reducción de tiempo y costos en transporte de los enfermos.
- Reducción de tiempo y costos en transporte de médicos, especialistas, etc.
- Reducción de costos en equipo.

2.1.4.6 Futuro

En la actualidad ya existen varias empresas que brindan este servicio, con la utilización básicamente de videoconferencias en tiempo real, sin embargo el futuro apunta a la utilización de la tele-presencia, de esta manera el médico será capaz de realizar cirugías remotamente.

2.1.5 VRVS [16]

2.1.5.1 Definición

VRVS (*Virtual Room Videoconferencing System*) significa "Sistema de Videoconferencia basado en Salas Virtuales". VRVS es una plataforma de colaboración entre personas geográficamente dispersas que funciona a través del sitio web: http://www.vrvs.org.

VRVS es un sistema basado principalmente en videoconferencias multipunto (dos o más personas comunicándose al mismo tiempo). Funciona bajo redes IP y soporta la mayoría de los sistemas operativos conocidos. VRVS es propiedad de Caltech (*California Institute of Technology*) y su uso está orientado únicamente a las comunidades educativas y de investigación en el mundo.

VRVS es una plataforma donde los usuarios pueden utilizar clientes H.323 para comunicarse. En el caso de las redes avanzadas utilizarán H.321 y H.310 ya que son los estándares a utilizarse sobre redes ATM.

La utilidad principal de este sistema es la comunicación entre estudiantes, profesores y/o investigadores que se encuentren separados geográficamente y necesiten colaborar entre ellos en cualquier momento y desde cualquier lugar.

2.1.5.2 Salas Virtuales

Una sala virtual es un espacio de reunión de un grupo de trabajo. Son espacios virtuales equivalentes a una sala de reuniones en una oficina. Básicamente es una página donde cada uno de los miembros del grupo aparecerá identificado con un ícono que llevará su nombre.

Las salas virtuales sirven para reunir a las personas en un día y hora en concreto, en la sala cada participante abrirá sus aplicaciones de video, para poder

comunicarse con el resto del grupo. Otras de las posibilidades dentro de una sala virtual es poder ofrecer el escritorio de un computador al resto de personas que se encuentran dentro de la sala.

2.1.5.2.1 Tipos de salas virtuales:

Salas de Pruebas. Estas salas no requieren reserva previa, pues siempre están abiertas, esto significa que en cualquier momento ser puede ingresar a ellas, hablar con alguien que se haya conectado o simplemente hacer pruebas enviando y recibiendo la propia voz e imagen.

Salas Privadas. Estas salas requieren reserva previa, a través del sistema de reserva del VRVS.

2.1.5.3 Sistema VRVS

El sistema VRVS se compone de dos partes:

2.1.5.3.1 Servidor Web

Servidor a donde los usuarios se conectan a las videoconferencias y lanzan sus aplicaciones.

2.1.5.3.2 Red de reflectores

Es una red mundial de reflectores interconectados que distribuyen los flujos de información a cualquier lugar desde donde el usuario se encuentre conectado.

Adicionalmente, la topología de reflectores en la red toma en cuenta tanto la geografía como el ancho de banda disponible para cada enlace de la red, esto para optimizar las rutas de comunicación.

Reflector: Un reflector es un equipo que interconecta a cada usuario hacia la sala virtual, por medio de un túnel IP permanente.

Un reflector es un PC con un software específico que ha sido desarrollado por VRVS.

Éste es encargado de enviar la información (audio, video, datos) entre los participantes de la videoconferencia.

El reflector es análogo a una Unidad de Control Multipunto.[3]

Cuando un usuario se conecta al sistema VRVS, su máquina queda asociada al reflector más próximo o al que tenga una mejor conexión. Siempre que el usuario envíe datos, video audio lo hará a través del reflector al cual se asoció, y siempre que reciba información igualmente lo hará a través del reflector asociado.

La asociación entre el usuario y el reflector depende de la ubicación física del usuario, es decir, cuando un usuario se conecta desde una parte geográficamente específica se asociará al reflector más cercano como ya se explicó, sin embargo, si el usuario cambia de ubicación geográfica por ejemplo en un país diferente la asociación se realizará con otro reflector.

---

[3] La función principal de un MCU es gestionar la comunicación entre diferentes terminales en un esquema de transmisión multipunto.[85]

En el proceso de registro, el usuario final se asocia automáticamente a su reflector más cercano. Cuando el usuario inicia una conexión con VRVS, el sistema envía una petición de conexión a su reflector, Si el reflector no responde, el usuario es conectado automáticamente al reflector de respaldo más cercano.

2.1.5.4 FUNCIONAMIENTO

Para utilizar el sistema se deben seguir los siguientes pasos:

2.1.5.4.1 Registrarse en el sistema

Ese proceso se lo realizará una sola vez, con la finalidad de obtener un *username* y un *password* los cuales se necesitan cada vez que se desee ingresar en el sistema para ello se tendrá que llenar un formulario con los datos personales y elegir a la comunidad a la que se desee pertenecer.

VRVS está dividido en comunidades. Cada comunidad tiene sus propias salas virtuales. Como usuarios del sistema se podrá entrar en cualquier sala virtual (siempre y cuando ésta no haya sido reservada con una clave de acceso).

Por otro lado solo se podrá reservar salas de la comunidad a la que se pertenezca como usuarios o salas de la comunidad *Universe* (Comunidad global por defecto del sistema).

2.1.5.4.2 Recibir confirmación vía correo electrónico

Se recibe una confirmación que llegará al buzón, el mensaje contendrá una clave y una dirección Web, se debe entrar en dicha dirección y colocar la clave proporcionada, con esto ya se quedará registrado en el sistema y se podrá tener acceso al mismo.

2.1.5.4.3 Bajar el software básico de VRVS

Una vez que se posee el *username* y el *password*, se debe bajar el *software* para el computador.

El sistema detecta automáticamente el tipo de sistema operativo que se está utilizando y muestra el *software* que se puede instalar.

2.1.5.5 Ventajas

La principal ventaja que brinda este sistema VRVS es la posibilidad de realizar reuniones en un mismo entorno virtual con personas geográficamente distribuidas. Los miembros de las salas generalmente pertenecen a una misma institución en particular, compañía, etc., de esta manera tienen un lugar de encuentro común en INTERNET.

2.1.6 SIMULACIÓN DISTRIBUIDA [17]

2.1.6.1 Definición

La simulación distribuida, como su nombre lo indica, es la realización de simulaciones repartidas entre diferentes máquinas de la red (todas parte de un mismo proyecto o actividad) obteniéndose un resultado final o conjunto de resultados los mismos que son presentados a los usuarios.

En la actualidad la realidad virtual que se desea simular ya sea con fines educativos, de entretenimiento, científicos etc., demanda grandes recursos computacionales, lo que resulta casi imposible de encontrar en una sola máquina.

Por este motivo nace esta nueva aplicación de simulación distribuida en donde el proceso de simulación se reparte entre varias máquinas de la red, obteniéndose

así mejores resultados, gracias al cambio de concepto sobre cómo y donde debe ser tratada la información que compone la base de la simulación y además al repartir la carga de procesamiento entre varios equipos.

2.1.6.2 Datos y Resultados

En cuanto al cómo y donde tratar la información, son criterios que se han modificado debido a que actualmente, se puede conseguir de manera fiable que un conjunto de equipos manejen la misma información y sean capaces de intercambiar resultados, casi simultáneamente.

En lo referente a la visualización de resultados en los procesos de simulación, lo que se encuentra a la orden del día es la utilización de lo que se denomina “Mundos Virtuales”. Realmente se trata de escenarios tridimensionales, visualizados en un *display* concreto, pero que se generan como combinación de procesos que se ejecutan en varias máquinas diferentes conectadas mediante una red de comunicaciones y por ello pueden ser tan complejos y completos como se desee.

En lo referente al manejo de información y su intercambio por los distintos elementos que van a realizar la simulación, también se plantean serios avances en los últimos años. Aunque el concepto de sistema distribuido es algo antiguo en la Informática, la estandarización de ciertos aspectos de los sistemas distribuidos es algo más actual, en concreto, lo que se refiere al intercambio de información para un propósito específico y de una manera determinada.

2.1.6.3 Estándares

En lo referente a simulaciones, se tiene SIMNET (*Simulator Networking*) un estándar para simulaciones distribuidas desarrollado a principio de 1985 bajo los auspicios de DARPA (*Defense Advanced Research Projects Agency*), cuya primera y principal aplicación fue con fines militares.

Posteriormente se desarrolla el estándar IEEE 1278.1 llamado DIS (*Distributed Interactive Simulation*) en 1995, que como su nombre indica es válido para simulaciones distribuidas interactivas. Ambos SIMNET y DIS, se entienden como protocolos que forman parte de la pila de protocolos que conforma la arquitectura de la red que se utiliza, aunque el segundo se apoya en TCP/IP y el primero no.

Además existen otros estándares, como HLA (*High Level Architecture*) o CAPE-OPEN (*Computer Aided Process Engineering Open Simulation Enviroment*), que dan una serie de especificaciones sobre los componentes, de modo que éstos puedan ser desarrollados y reutilizados por terceras personas fácilmente.

2.1.6.4 Sistema

En el proceso de Simulación se pueden distinguir tres partes:

- **Lenguajes de Simulación**. Plataforma y lenguaje en que se va a desarrollar el sistema.

- **Intercambio de Información**. Intercambio de información (datos, variables, etc.) debe ser en tiempo real a través de redes de alta velocidad.

- **Generación de gráficos**. Generación de gráficos que presenten resultados, igualmente debe ser desarrollado en algún lenguaje de programación.

2.1.6.5 Recursos

Obviamente, la simulación en tiempo real es una cuestión ya conocida, ampliamente estudiada y en la que el problema fundamental no es la complejidad

de los algoritmos que se utilicen para representar el modelo, sino la potencia del computador sobre el que se ejecuta la simulación, que condiciona aspectos fundamentales como son la visualización de resultados en tiempo real, la posibilidad de modificar parámetros de ejecución en función de los resultados parciales que se obtienen y si la escala de tiempo simulado se corresponde con la realidad.

Las simulaciones en tiempo real son firmes candidatos a utilizar este tipo de sistemas, ya que se puede repartir la potencia de cálculo entre las diferentes CPU´s que conformen el sistema distribuido, utilizando la red de comunicación para intercambiar información entre los distintos procesos que se ejecutan. Configurando adecuadamente la simulación se pueden obtener los resultados de cada instante simulado y por último su representación gráfica que representa el comportamiento del sistema en el tiempo.

2.1.6.6 Ventajas

La aplicación trae grandes ventajas a todo nivel. Es así que en el campo del entretenimiento se aplica este proceso para simulación de ambientes virtuales para la creación de escenarios ficticios en una película por ejemplo.

En el ámbito educativo es de gran ayuda pues se podrán realizar experimentos complejos gracias a la distribución de simulación del sistema y como usuario se está limitado a recibir resultados de manera transparente.

2.1.6.7 Futuro

La aplicación se encuentra en total desarrollo, desde la aparición de las redes avanzadas de alta velocidad, se espera modelar procesos muy complejos, creación de realidades virtuales con las que el usuario pueda interactuar como parte de ellas, aunque aún se depende de otros avances de la electrónica el futuro de la aplicación tiene grandes objetivos y expectativas por cumplir.

2.1.7 *LEARNINGWARE* [18]

2.1.7.1 Definición

Sistema de gestión instructiva que involucra el desarrollo de material educativo y su distribución sobre redes públicas o privadas.

Conceptualmente, los profesores y estudiantes pueden compartir materiales en el ciberespacio. Los alumnos aprenden de un modo autodirigido bajo la supervisión de un sistema educativo o *software* de aprendizaje.

2.1.7.2 Aprendizaje Asincrónico

En un sistema de enseñanza grupal todos los aprendices tienen distintos ritmos de aprendizaje, en una aula el profesor visualiza esta situación y toma medidas para conservar el ritmo de aprendizaje individual y del grupo.

Sin embargo, si los aprendices se encuentran distantes y haciendo uso de una plataforma LMS (*Learning Managment System*), deben existir herramientas que le permitan al tutor o guía del proceso de aprendizaje, conocer de forma automática el avance individual y del grupo para tomar acciones del caso.

2.1.7.3 LMS

La aparición de una gran cantidad de *software* de aprendizaje o *learningware* ha dado origen por una parte a nuevos enfoques metodológicos en la construcción de *software*, como es el caso de los objetos de aprendizaje, plataformas computacionales de apoyo como son los sistemas administradores de aprendizaje o LMS y estándares como es el caso de SCORM (*Sharable Content Object Reference Model*).

En los últimos años los sistemas administradores de aprendizaje o LMS son *software* que proveen a profesores y aprendices espacios virtuales para la enseñanza-aprendizaje, es decir la capacidad de administrar programas o cursos completos a través de mantener material necesario para el aprendizaje, administrar usuarios, recursos y también herramientas de comunicación como pizarras, *chats*, foros, calendario de actividades, etc.

Por otra parte si se considera un LMS como un sistema distribuido de computación, donde cada uno de los aprendices es asociado a un proceso de aprendizaje. El curso basado en objetos de aprendizaje en donde la superación de cada uno de ellos es marcado como un “evento de aprendizaje” y la velocidad con que cada aprendiz desarrolla su propio proceso se asocia a un “reloj virtual de aprendizaje”.

Se puede desarrollar un modelo de aprendizaje asincrónico basado en objetos de aprendizaje sobre un LMS de código abierto que haga uso de algoritmos de *multicast* en sistemas distribuidos.

El diseño de un LMS es una tarea compleja y requiere de conocimientos en educación, psicología e informática, en particular en sistemas distribuidos de computación.

Además, debe contener adecuados formatos en la presentación de la información, la facilidad de lectura y comprensión deben primar sobre otras consideraciones.

- Eliminación de las referencias externas al propio objeto, en un objeto de aprendizaje que debe ser auto-contenido no se admiten llamadas para que el lector revise capítulos anteriores. Este tipo de información la debe incluir el integrador en el momento de contextualizar el curso.

- Consistencia en el uso del lenguaje, meditada elección de la terminología evitando la utilización de sinónimos que induzcan a confusión.

- Lenguaje apropiado para una gran audiencia huyendo de la excesiva especialización.

- Eliminación de los textos densos que dificultan la lectura en pantalla, en la mayoría de los casos los objetos de aprendizaje se consumen vía *web* y por tanto la presentación de la información deberá estar preparada para ello.

Los LMS poseen una serie de características, entre ellas tenemos:

- **Número de usuarios**. Es decir el número de aprendices posibles de administrar, normalmente este número es lo suficientemente alto como para dar soporte a cualquier programa educacional. Depende mas bien del tamaño del servidor y de la base de datos.

- **Tipo de Servidores**. Existen LMS disponibles para versiones de Windows, LINUX y ambas.

- **Bases de Datos**. Las cuales generalmente son del tipo Oracle, o SQL (*Structured Query Language*).

- **Especificación de E-*Learning***. Es probablemente una de las características más importantes en la actualidad y está referida al tipo de certificación SCORM.

- **Herramientas de instrucción de salas reales y virtuales**. Esta característica está referida a la posibilidad de administrar en tiempo real recursos en una sala de clases, como cámaras de video, equipos retroproyectores, etc.

- **Colaboración**. La mayoría de los LMS cuentan con la posibilidad de conversación en línea (*chat*) y foros, este último entendido como el seguimiento de una discusión respecto de un tema, además de la posibilidad de formar grupos de trabajo. Sin embargo, sólo unos pocos tienen incluido un servicio de correo electrónico, la mayoría registra usuarios los cuales tienen sus propias cuentas de correo en servidores externos, muchas veces públicos.

- **Multi-idioma**. Una característica importante es la posibilidad de manejar varios idiomas y múltiples caracteres. Es decir, con la posibilidad de personalizarlos al momento de su instalación. Esta característica la tienen generalmente los LMS desarrollados en países con otras formas de escritura.

- **Creación y Administración de Contenidos**. Básicamente se refiere a si tiene características de sistemas administradores de contenidos de aprendizaje o LCMS (*Learning Content Manangment System*), las cuales están referidas a si tienen la capacidad adicional de crear contenidos.

2.1.7.4 LCMS

Una de las aplicaciones más importantes para la administración del conocimiento y el aprendizaje son los LCMS. Mientras que un LMS es un sistema que permite organizar estudiantes y eventos de capacitación, así como dar seguimiento al aprendizaje, un LCMS permite además administrar la creación, almacenamiento,

reutilización y distribución de contenido, desde un repositorio central de objetos de aprendizaje accesible a las personas que lo requieran en el momento indicado.

Los LCMS frecuentemente hacen separación de contenidos, los cuales son tratados para su presentación con XML. Esto permite que muchos LCMS puedan publicar a un amplio rango de formatos, plataformas o dispositivos como impresoras e inclusive dispositivos de información inalámbrica o WID (*Wireless Information Devices*) tales como *Palm* y *handhelds.*

Los LCMS son ambientes estructurados diseñados para que las organizaciones puedan implementar mejor sus procesos y prácticas con el apoyo a cursos, materiales y contenidos en línea. Permiten una creación mucho más eficiente, evitan redundancia y permiten administrar también la participación de diversos desarrolladores, expertos colaboradores o instructores que participan en la creación de contenidos.

Estos LCMS representan la integración de dos vías tradicionalmente separadas: Los CMS (*Content Management System*) y los LMS. Estos dos mundos se han desarrollado independientemente. El aprendizaje a través de la red necesariamente requiere de recursos que permitan tanto la creación como la distribución de contenidos integrados en una misma plataforma.

Desde el punto de vista de las definiciones anteriores un LCMS debería contener las siguientes herramientas adicionales a un LMS:

1. Herramientas para la administración del sistema que permita las matrículas, el uso de los tiempos, el seguimiento del aprendizaje de los usuarios, la adecuación de los contenidos, etc.

2. Herramientas para la evaluación continua a lo largo del curso, el sistema debe proveer de recursos suficientes para valorar los aprendizajes bajo distintos niveles de dificultad y diferentes modalidades de medición.

2.1.7.5 Ventajas

La existencia de un sistema que maneja de educación a distancia basado en estándares internacionales, que involucran aspectos como pedagogía, evaluación, etc., es decir, que no son meramente técnicos, garantizan un alto nivel de enseñanza permitiendo así al estudiante:

- Tener una fuente complementaria, autosuficiente de información.
- Acceso en cualquier momento.
- Evaluación y chequeo de progreso.
- Auto educación.
- Bibliografía ilimitada y bien organizada, entre otras.

2.1.8 NUEVAS APLICACIONES

Con la infraestructura que poseen las redes avanzadas se da la posibilidad del surgimiento de nuevas aplicaciones que están en desarrollo en la actualidad y que han sido orientadas al ámbito educativo, de entre ellas se puede mencionar como relevante a:

Astronomía. Acceso a recursos remotos, como telescopios. Con esta aplicación no hace falta que el observador esté frente a un telescopio, ya que el instrumento de observación captura datos y los envía por la red, llegando al observador final el cual puede manipular los datos digitalmente.

2.2 ANÁLISIS DE LOS PRINCIPALES PROTOCOLOS UTILIZADOS POR LAS APLICACIONES

2.2.1 *MULTICAST* [19][20]

2.2.1.1 Definición

Es una tecnología con la cual se realiza el envío de la información en una red a múltiples destinos simultáneamente. Un único flujo de datos, proveniente de una determinada fuente, se puede enviar simultáneamente a varios receptores.

2.2.1.2 Estado actual con *Unicast*

Unicast es el envío de información desde un único emisor a un único receptor.

TCP está orientado a *unicast*. UDP soporta muchos otros paradigmas, pero si se lo utiliza en la transferencia de información desde un único emisor hacia un único receptor, es también *unicast*.

Las transmisiones *unicast* eran suficientes para Internet. Sin embargo con el pasar del tiempo, la información de la *web* empezó a incorporar nuevos elementos, tal es el caso de imágenes, audio, video, etc.

Si se deseaba enviar audio y vídeo, que necesitan de un gran ancho de banda comparado con aplicaciones *web*, se tenía dos opciones:

- Establecer conexiones *unicast* por separado con cada uno de los receptores, ó
- Usar *broadcast*.

La primera solución no era factible, ya que cada conexión enviando audio y vídeo consume una gran cantidad de ancho de banda, establecer cientos, quizás miles de estas conexiones provocarían un colapso en la red.

La segunda solución *broadcast* es aparentemente una salida a la problemática presentada, pero desde luego no es la solución. Si deseara que todos los computadores en la LAN (*Local Area Network*) atendieran la conferencia, se podría utilizar *broadcast*. Se enviarían los paquetes una sola vez y cada máquina en la LAN lo recibiría ya que fueron enviados a la dirección de *broadcast*.

El problema es que quizás solo algunos de éstos y no todos estén interesados en estos paquetes. Más aún, quizás algunos computadores deseen los datos pero están fuera de la LAN a varios enrutadores de distancia, en este caso la información no llegaría pues los enrutadores dividen la red en dominios de *broadcast* y no permitirían el paso de la información hacia las otras redes.

La mejor solución parece ser aquella en la que sólo se envían paquetes a ciertas direcciones especiales. Así, todos los computadores que han decidido unirse a la conferencia conocerán la dirección de destino, esto es similar al *broadcast* en el sentido de que sólo se envía un paquete de *broadcast* y todos los computadores en la red lo reconocen y lo leen, difiere sin embargo, en que no todos los paquetes de *multicast* son leídos y procesados, ya que solo lo harán los computadores interesados.

2.2.1.3 Direcciones *Multicast* [19]

En IPv4, se reserva las direcciones de tipo D para la multidifusión. (224.0.0.0 a 239.255.255.255).

Hay algunos grupos especiales de *multicast*, o grupos de *multicast* bien conocidos y no se debería usar ninguno de éstos en una aplicación determinada dado que están destinados a un propósito en particular:

224.0.0.1: Es el grupo de todos los computadores. Si hace un *ping* a ese grupo, todos los computadores que soporten *multicast* en la red deben responder, ya que todos ellos deben unirse a este grupo en el arranque de todas sus interfaces que soporten *multicast*.

224.0.0.2: Es el grupo de todos los enrutadores. Todos los enrutadores de *multicast* deben unirse a este grupo en todos las interfaces de *multicast*.

224.0.0.4: Es el de todos los enrutadores DVMRP (*Distance Vector Multicast Routing Protocol*).

224.0.0.5: Es el de todos los enrutadores OSPF (*Open Short Path First*).

224.0.0.13: Es el de todos los enrutadores PIM (*Protocol Independent Multicast*).

En cualquier caso, el conjunto de direcciones de la 224.0.0.0 a 224.0.0.255 están reservadas localmente para tareas administrativas y de mantenimiento y los paquetes enviados a éstos nunca se envían a los enrutadores *multicast*. De manera similar, el conjunto 239.0.0.0 a 239.255.255.255 ha sido reservado para ámbitos administrativos.

En IPv6 se reserva la dirección ff::[4]

2.2.1.4 Nivel de cumplimiento [19]

Los computadores pueden estar en tres niveles:

Se está en **Nivel 0** cuando no hay soporte para *multicast* en IP (*Internet Protocol*). Un buen número de los computadores y los enrutadores de Internet están en este nivel, ya que el soporte de *multicast* no es obligatorio en IPv4 (sí lo es, sin embargo, en IPv6). Los computadores en este nivel no pueden enviar ni recibir paquetes *multicast*. Deben ignorar los paquetes enviados por otros computadores con capacidades de *multicast*.

En el **Nivel 1** hay soporte para envío pero no para recepción de paquetes IP de *multicast*. Nótese, por tanto, que no es necesario unirse a un grupo *multicast* para enviar paquetes.

El **Nivel 2** es el de completo soporte a *multicast* en IP. Los computadores de nivel 2 deben ser capaces de enviar y recibir tráfico *multicast*. Tienen que saber la forma de unirse o dejar grupos *multicast* y de propagar esta información a los enrutadores *multicast*. Es necesario incluir, por tanto, una implementación del Protocolo de Gestión de Grupos de Internet (Internet Group Management Protocol, IGMP) en su pila TCP/IP.

---

[4] Más adelante se indica el direccionamiento *multicast* en Ipv6

2.2.1.5 MRouter

Para que la información se propague hacia segmentos fuera de la red local se utilizan los enrutadores que interconectan tanto múltiples segmentos de red, como las múltiples redes que forman Internet. Cuando un enrutador está calificado para intercambiar paquetes IP *multicast* con otro u otros, decimos que es un enrutador *multicast*, o abreviadamente un m*router*.

Un *mrouter* debe cumplir dos requisitos básicos:

- Debe tener un mecanismo para conocer en todo momento los equipos que pertenecen a un determinado grupo *multicast* en cada una de las redes que interconecta.

- Para cada pareja {dirección IP origen (o fuente), grupo *multicast*} debe saber cómo encaminar los paquetes, originados en esa dirección IP, a los segmentos de red donde haya otros miembros de ese grupo.

Lo primero se consigue con un determinado diálogo entre *mrouters* y computadores según un determinado lenguaje, o técnicamente, un protocolo de comunicaciones. Este protocolo es el IGMP (*Internet Group Management Protocol*), que debe implementar cualquier equipo que hable *multicast* (computadores y *mrouters*).

Lo segundo se refiere a los criterios de encaminamiento *multicast* MRP (*Multicast Routing Protocols*) de los que debe disponer el *mrouter*, y que se presentará en la siguiente sección.

2.2.1.6 Protocolos de enrutamiento *Multicast* [20]

Para poder informar a otros enrutadores sobre fuentes y destinos de *multicast* se deben emplear protocolos de enrutamiento. Existen tres categorías básicas:

- **Protocolos de Modo Denso:** DVMRP (*Distance Vector Multicast Routing Protocol*) y PIM-DM (*Protocol Independent Multicast Dense Mode*).

- **Protocolos de Modo *Sparse:*** PIM-SM (*Protocol Independent Multicast Sparce Mode*) y CBT (*Core-Based Trees*).

- **Protocolos de Estado de Enlace:** MOSPF (*Multicast Open Short Path First*).

Los protocolos de modo denso como DVMRP y PIM-DM utilizan el árbol más corto junto con un mecanismo de empuje. Este mecanismo de empuje asume que en cada interfaz del enrutador existe al menos un receptor del grupo.

El tráfico es enviado a través de todas las interfaces (*flood*). Para evitar el desperdicio de recursos, si un enrutador no desea recibir tráfico envía un mensaje de supresión (*prune*). Como resultado se tiene que el tráfico de *multicast* sólo es enviado a los enrutadores que tienen miembros de grupos de *multicast*.

Este comportamiento de "*Flood*" y "*Prune*" se repite aproximadamente cada 2 o 3 minutos dependiendo del protocolo, por esta razón protocolos del tipo denso son mayormente empleados en ambientes LAN y donde el número de receptores usualmente es alto comparado con el de las fuentes y donde el ancho de banda no es un factor restrictivo.

Los protocolos del tipo *Sparse* hacen uso del modelo de árboles compartidos, al contrario de los DM (*Dense Mode*), los SM (*Sparce Mode*) hacen uso de un mecanismo de hale. Este mecanismo asume que no existen receptores interesados en el tráfico de *multicast*, de esta forma ningún tráfico es enviado a menos que exista una solicitud explícita.

Para que el árbol compartido sea construido, el enrutador receptor debe enviar a la raíz una solicitud de unión al árbol (*Join message*). Este mensaje viaja de enrutador a enrutador construyendo a su paso el camino hacia la raíz. Cuando un receptor desea dejar de recibir tráfico, debe enviar un mensaje de supresión (*Prune*) al igual que lo hacen los DM.

Por su mecanismo de hale, los protocolos SM son utilizados en ambientes WAN donde el ancho de banda es escaso o cuando se tienen más fuentes que destinos.

El punto más crítico de estos protocolos es el RP *Rendezvous Point*[5] ya que si éste no está bien ubicado por el administrador de la red puede ocasionar que el camino fuente-destino no sea el óptimo o que por exceso de tráfico el RP se convierta en un “cuello de botella”. PIM-SM cuenta con un mecanismo que permite conmutar de árbol compartido a SPT (*Short Path First*) para una fuente en particular.

Los protocolos de estado de enlace como MOSPF hacen uso del SPF para construir estos árboles, los enrutadores envían información de estados de enlace que identifica la ubicación en la red de los grupos de miembros de *multicast*. Con

---

[5] Un RP es un enrutador que actúa como lugar de encuentro para las fuentes y receptores de datos *multicast.*

esta información los enrutadores forman un SPT de cada fuente hacia todos los receptores en el grupo.

2.2.1.7 Ventajas

La ventaja de IP *multicast* es la transmisión de información en tiempo real para múltiples receptores. En estos casos la utilización del *multicast* permite un ahorro substancial de los recursos de red consumidos y por ende una mejora en la transmisión de esta información y una mejor relación calidad/costo. La ventaja de aprovechar el *multicast* para la transmisión de datos multimedia frente a las comunicaciones uno a uno, es el ahorro de recursos telemáticos y por tanto la eficiencia de las aplicaciones a iguales gastos en infraestructura.

2.2.2 IPV6 [21]

2.2.2.1 Definición

IPv6 (también conocido como IPng o “IP de nueva generación”) es la nueva versión del conocido protocolo de red IP, también llamado IPv4. IPv6 se puede instalar como una actualización de *software* y es capaz de trabajar con el actual protocolo IPv4.

2.2.2.2 Por qué IPv6

Al comienzo de los años 90 dada la expansión de Internet, rápidamente se empezó a consumir el espacio de direcciones de IPv4, aunque después se solucionó de alguna manera este problema con la utilización del espacio de direccionamiento privado junto con NAT (Network Address Traslation).

IPv6 ofrece un espacio de direccionamiento de 128 bits en teoría existen 340 282 366 920 938 463 463 374 607 431 768 211 456 direcciones disponibles en

comparación a IPv4 que ofrece teóricamente un espacio de 4 294 967 296 direcciones.

2.2.2.3 Cabecera IPv6

Véase en primer lugar la descripción de la cabecera IPv4 en la figura 2.5:

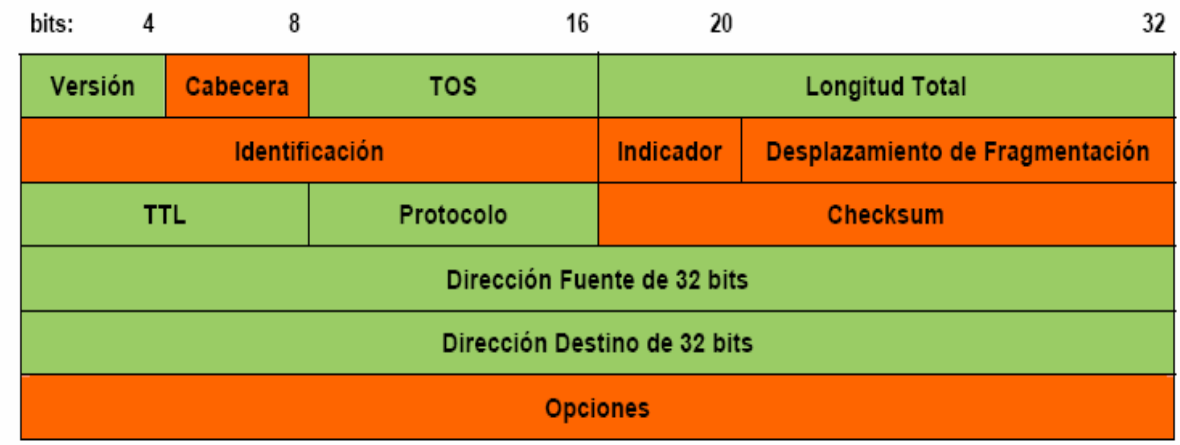


Figura 2.5 Cabecera IPv4 [21]

La longitud mínima de la cabecera es de 20 bytes (cada fila de la tabla supone 4 bytes) a ello hay que añadir las opciones[6] que dependan de cada caso.

En la tabla anterior se han marcado mediante el color de fondo los campos que van a desaparecer y los que se han modificado en IPv6.

[6] El campo opciones se rellena para completar múltiplos de cuatro bytes. Actualmente hay cinco opciones definidas, aunque no todos los encaminadores las reconocen: Seguridad, Enrutamiento estricto desde el origen, Enrutamiento libre desde el origen,Registrar ruta y Marca de tiempo. [86]

Se pasa de tener 12 campos en IPv4 a 8 en IPv6.

El motivo de la eliminación de los campos es la innecesaria redundancia. En IPv4 se facilita la misma información de diferentes formas. Por ejemplo el campo *checksum* o de verificación de la integridad de la cabecera. Otros mecanismos de encapsulado ya realizan esta función. Por ejemplo IEEE 802 MAC, *framing* PPP (*Point to Point*), capa de adaptación ATM (*Asynchronous Transfer Mode*).

El caso del campo de "Desplazamiento de Fragmentación", es ligeramente diferente, dado que el mecanismo por el que se realiza la fragmentación de los paquetes es totalmente modificado en IPv6, lo que implica la total inutilidad de este campo. En IPv6 los enrutadores no fragmentan los paquetes, sino que de ser precisa la fragmentación des-fragmentación se produce extremo a extremo.

Algunos de los campos son renombrados:

Longitud total: Longitud de carga útil (*payload length*), que en definitiva es la opción de los propios datos y puede ser de hasta 65.536 *bytes*. Tiene una longitud de 16 *bits* (2 *bytes*).

Tiempo de vida: Límite de saltos (*Hop Limit*). Tiene una longitud de 8 *bits* (1 *byte*).

TOS (*Type Of Service*): Clase de tráfico (*Traffic Class*), también denominado Prioridad (*Priority*) o simplemente Clase (*Class*), Tiene una longitud de 8 *bits* (1 *byte*).

Los nuevos campos son:

Siguiente cabecera: (*next header*), dado que en lugar de usar cabeceras de longitud variables se emplean sucesivas cabeceras encadenadas, de ahí que desaparezca el campo de opciones. En muchos casos ni siquiera es procesado por los enrutadores, sino tan solo extremo a extremo. Tiene una longitud de 8 *bits* (1 *byte*). Este campo reemplaza al campo Protocolo de IPv4

Etiqueta de flujo: Para permitir tráficos con requisitos de tiempo real. Tiene una longitud de 20 *bits*.

Los campos Clase de Tráfico y Etiqueta de Flujo son los que permiten una de las características fundamentales e intrínsecas de IPv6. Calidad de Servicio (*Qos*), Clase de Servicio (*Cos*) y en definitiva un poderoso mecanismo de control de flujo, de asignación de prioridades diferenciadas según los tipos de servicios.

El valor del campo "**siguiente cabecera**" como su nombre lo indica muestra la siguiente cabecera y así sucesivamente. Las sucesivas cabeceras no son examinadas en cada nodo de la ruta, sino solo en el nodo o nodos destinos finales.

Hay una única excepción a esta regla, cuando el valor de este campo es cero, lo que indica opción de examinado y proceso salto a salto. Se pueden citar algunos ejemplos: Cabeceras con información de encaminado, fragmentación, opciones de destino, autenticación, encriptación, etc., que en cualquier caso deben ser procesadas en el orden riguroso en el que aparece el paquete.

Por tanto en IPv6 la cabecera tiene el siguiente formato:

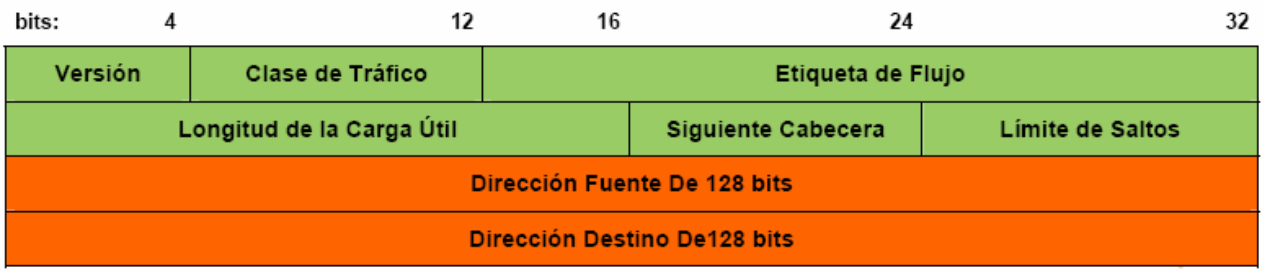


Figura 2.6 Cabecera IPv6 [21]

La longitud de esta cabecera de es de 40 *bytes*, el doble en el caso de IPv4, pero con muchas ventajas al haberse eliminado campos redundantes.

Además la longitud fija de la cabecera, implica una mayor facilidad para su procesamiento en enrutadores y conmutadores, incluso mediante *hardware*, lo que implica mayores prestaciones.

Ejemplos de cabeceras de extensión:

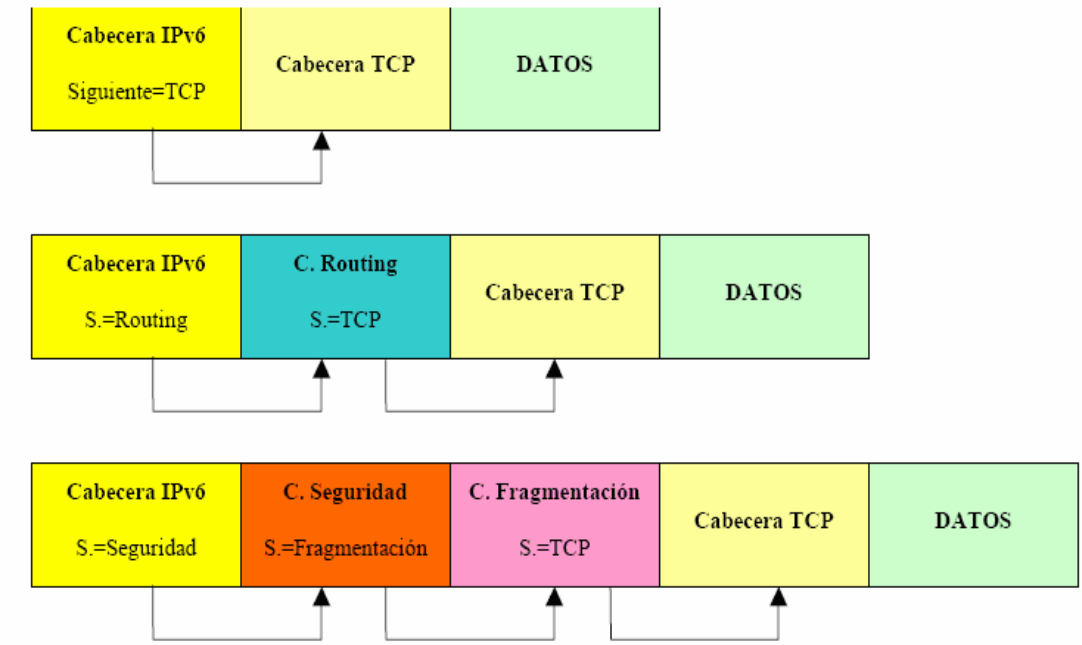


Figura 2.7 Cabeceras de Extensión

El MTU (*Maximum Transmission Unit*) debe ser como mínimo de 1.280 *bytes*, aunque se recomiendan tamaños superiores de 1500 *bytes*. Los nodos descubren el valor del MTU a través de la inspección de ruta. Se provee así una optimización de los paquetes y del número de cabeceras, dado el continuo crecimiento de los anchos de banda disponibles, así como del intercambio del propio tráfico.

Dado que IPv6 no realiza verificación de errores en la cabecera, en tráfico UDP se requiere el empleo de su propio mecanismo de *checksum*.

2.2.2.4 Tipos de direcciones IPv6

2.2.2.4.1 Definición de direcciones IPv6

Las direcciones IPv6 son identificadores de 128 *bits* de longitud. Identifican interfaces de red (ya sea de forma individual o grupos de interfaces). A una misma interfaz de un nodo se le pueden asignar múltiples direcciones IPv6 dichas direcciones se clasifican en tres tipos.

***Unicast*:** Identificador para una única interfaz. Un paquete enviado a una dirección *unicast* es entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4.

***Anycast*:** Identificador para un conjunto de interfaces (típicamente pertenecen a diferentes nodos). Un paquete enviado a una dirección *anycast* es entregado en una (cualquiera) de las interfaces identificadas con dicha dirección (la que esté más cerca). Nos permite crear, por ejemplo, ámbitos de redundancia, de forma que varias máquinas pueden ocuparse del mismo tráfico según una secuencia determinada por el *routing* si la primera cae.

***Multicast*:** Identificador para un conjunto de interfaces (por lo general pertenecientes a diferentes nodos). Un paquete enviado a una dirección *multicast* es entregado a toda las interfaces identificadas por dicha dirección. La misión de este tipo de paquetes es evidente, aplicaciones de retransmisión múltiple.

Una dirección *multicast* en IPv6, puede definirse como un identificador para un grupo de nodos. Un nodo puede pertenecer a uno o varios grupos *multicast*.

Las direcciones *multicast* tienen el siguiente formato:

8	4	4	112 bits
11111111	000T	ámbito	Identificador de Grupo

Los primeros 8 *bits* indican que se trata de una dirección *multicast*, el *bit* "T" indica:

"T" = 0 indica una dirección permanente, asignada por la autoridad enumeración global del Internet.

"T" = 1 indica una dirección temporal.

Los *bits* "ámbito" tienen los siguientes significados:

0 Reservado
1 Ámbito local de Nodo
2 Ámbito local de enlace
3 No asignado
4 No asignado

5	Ámbito local de sitio
6	No asignado
7	No asignado
8	Ámbito local de organización
9	No asignado
A	No asignado
B	No asignado
C	No asignado
D	No asignado
E	Ámbito global
F	Reservado

Tabla 2.1 Significado de los bits del campo “ámbito” de la dirección *Multicast*

2.2.3 PROTOCOLOS Y ESTÁNDARES PARA VIDEOCONFERENCIA

	H.320	**H.321**	**H.322**	**H.323**	**H.324**
Fecha	1990	1995	1995	1996	1996
Red	RDSI-BE	RDSI-BA ATM LAN	X.25	LAN Ethernet ATM	RTB
Vídeo	H.261 H.263	H.261 H.263	H.261 H.263	H.261 H.263	H.261 H.263
Audio	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.723 G.728 G.729	G.723
Datos	T.120	T.120	T.120	T.120	T.120

Multiplexación	H.221	H.221	H.221	H.225	H.223
Control	H.230 H.242	H.242	H.230 H.242	H.245	H.245
Multipunto	H.231 H.243	H.231 H.243	H.231 H.243	H.323	XXX

Tabla 2.2 Normativa de la UIT para conferencia multimedia sobre redes LAN y WAN [23]

En las redes avanzadas debido a que operan con ATM podemos utilizar H.321 o H.323

2.2.3.1 ITU-T *Recommendation* H.321: *Adaptation of* H.320

Esta recomendación define cómo adaptar los terminales H.320 para que trabajen en entornos RDSI (Red Digital de Servicios Integrados).

- Sigue especificando el uso de los estándares G.711 para el sonido y H.261 para el vídeo.

- Por una parte, se impone que el ancho de banda máximo a utilizar para el vídeo sea 2 Mbps (el límite de H.261).

- También se impone el uso del AAL1 (*ATM Adaptation Layer 1*), lo que es una limitación, porque un sistema de videoconferencia podría aprovechar de forma óptima un servicio VBR (*Variable Bit Rate*), dadas las características del tráfico que genera.

2.2.3.2 ITU-T *Recommendation* H.323

Es una recomendación del ITU (*International Telecommunication Union*), que define los protocolos para proveer sesiones de comunicación audiovisual, sobre una red de conmutación de paquetes.

Especifica los ya conocidos estándares H.261, G.711 y T.120 para el vídeo, el audio y los datos, por motivos de compatibilidad entre otros. Como formatos alternativos, se citan el H.263 para vídeo, y los G.722, G.723, G.728 y G.729 para audio.

El intercambio de información de manera fiable (por ejemplo, los datos y la información de control) se realiza bajo TCP. La transmisión de paquetes de sonido y vídeo se realiza bajo UDP, para evitar la sobrecarga de TCP.

Entre los componentes más relevantes que el estándar define se tiene:

Terminal

Son los clientes finales, que proporcionan una comunicación bidireccional en tiempo real.

Gateway

Un *gateway* permite conectar una red H.323 con otra red no H.323. Sus dos funciones básicas son las de traducir los distintos protocolos de establecimiento y fin de llamada empleados por las distintas redes, y realizar la conversión de formatos de audio y vídeo.

Gatekeeper

El *gatekeeper* se puede considerar el punto central en una red H.323 y define el concepto de zona H.323. Una zona es un conjunto de MCUs (Unidades de Control Multipunto), *gateways* y terminales gestionados principalmente por un *gatekeeper*.

Los *gatekeepers* no son necesarios para llamadas entre terminales H.323 dentro de una misma red, aunque sí lo son cuando se desea compatibilidad con las redes de telefonía.

Unidad de Control Multipunto (MCU)

La MCU está encargada de dar soporte a las conferencias entre tres o más puntos finales H.323. Una MCU consta de un controlador multipunto (MC) y uno o más procesadores multipunto (MP).

El MC se encarga de transmitir información de los *codecs* soportados por los distintos terminales para poder así negociar los *codecs* de audio y vídeo utilizados durante la conferencia.

Los MPs, por su parte, distribuyen los flujos de audio, datos, vídeo entre los distintos terminales que participan en una multiconferencia.

3 DISEÑO DE LA INFRAESTRUCTURA DE RED DE LOS MIEMBROS DE CEDIA

3.1 ANÁLISIS DEL TRÁFICO QUE GENERAN LAS APLICACIONES

3.1.1 TRÁFICO GENERADO POR CADA APLICACIÓN

- Bibliotecas digitales

  Una biblioteca digital contiene todo tipo de material que una biblioteca tradicional posee, pero en formato digital, así se tiene:

  - Datos
  - Video y audio en tiempo no real

- Teleinmersión

  Debido a que esta aplicación no se encuentra implementada en la actualidad en la red avanzada ecuatoriana, se tomarán valores referenciales de entidades que han realizado el análisis de tráfico respectivo, para tener un valor estimado del consumo de capacidad.

- Laboratorios Virtuales

  En un laboratorio virtual, se puede observar tráfico de:

  - Datos
  - Audio en tiempo real
  - Video y audio en tiempo no real

- Telemedicina

  En telemedicina, existe tráfico de:

  - Datos
  - Videoconferencia

- VRSV

  En el sistema de videoconferencia basado en salas virtuales, existe tráfico de:

  - Datos
  - Videoconferencia

- *Learningware*

  En *learningware* , se puede observar tráfico de:

  - Datos
  - Video y audio en tiempo no real

- Simulación Distribuida

  En simulación distribuida , se puede observar tráfico de:

  - Datos

3.1.2 ANÁLISIS DE TRÁFICO QUE GENERAN LAS APLICACIONES

Para realizar el análisis de tráfico, existen a disposición una gran variedad de soluciones que van desde productos propietarios que incluyen *hardware* y *software*, hasta soluciones gratuitas y de código abierto.

Para efectos de este análisis se utilizará la aplicación Ethereal.

Ethereal

Es un potente analizador de protocolos de redes, sus bases residen en la librería “pcap” diseñado para máquinas Unix y Windows. Permite capturar datos directamente de una red u obtener información a partir de una captura en disco (puede leer más de 20 tipos de formato distintos). Destaca también por su soporte de más de 300 protocolos.

Para lograr el objetivo planteado se utilizarán las siguiente topologías.

Para el análisis de datos:

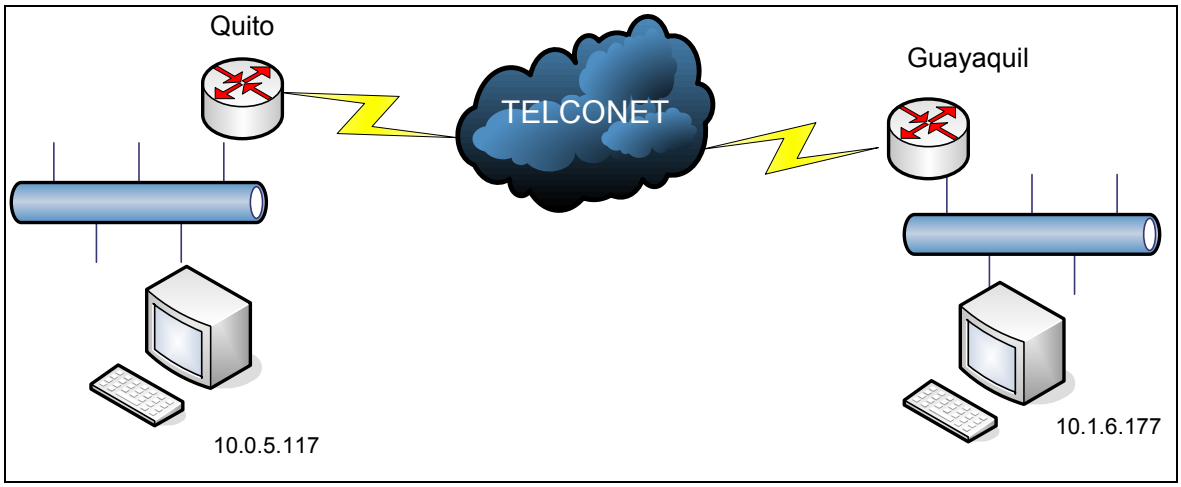


Figura 3.1 Diagrama de red de pruebas para tráfico de datos

Para el análisis de videoconferencia:

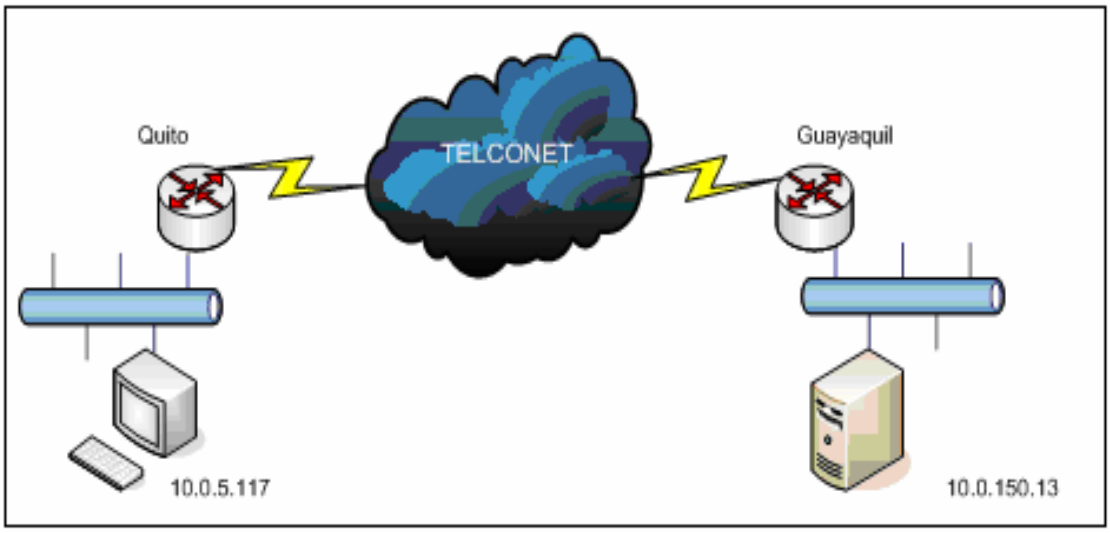


Figura 3.2 Diagrama de red de pruebas para tráfico de videoconferencia

Para descarga de archivos y navegación a través del Internet comercial:

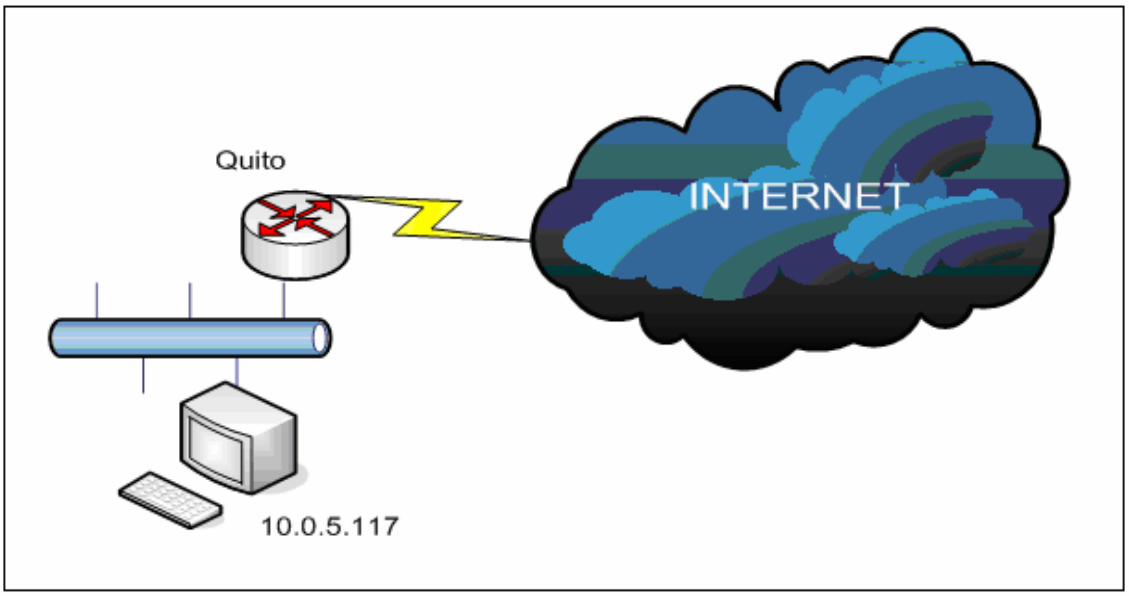


Figura 3.3 Diagrama de red de pruebas para navegación por Internet

Para el análisis del tráfico de datos, se utiliza un computador con dirección IP 10.0.5.117 ubicado en Quito y otro ubicado en Guayaquil con dirección IP 10.1.6.177.

Para el análisis del tráfico de videoconferencia, se utliza un computador con dirección IP 10.0.150.13, que posee la herramienta *Microsoft Office Communicator*, ubicado en Guayaquil y un computador ubicado en Quito con dirección IP 10.0.5.117.

En el caso del análisis de tráfico a través del Internet comercial, las pruebas se realizarán en un enlace dedicado de 350 Kbps contratados con Telconet.

Los equipos de Quito y Guayaquil se encuentran enlazados a través de una conexión dedicada provista por Telconet y las últimas millas tienen una capacidad contratada de 1 Mbps.

Se ha realizado el análisis sobre este enlace, debido a su similitud en cuanto a la capacidad de 1 Mbps, que es la mínima contratada por un miembro tipo de CEDIA para la red avanzada y además porque se encuentra sobre la red de Telconet, con lo que se espera se tendrán características similares de transmisión.

Se debe recalcar que, aunque en la red avanzada se utiliza direccionamiento IPv6, los paquetes IPv6 son encapsulados en paquetes IPv4 en los equipos de Telconet, razón por la cual el análisis se lo realiza sobre IPv4 con el fin de obtener un valor aproximado de capacidad consumida por cada aplicaión.

3.1.2.1 Pruebas y resultados

Las consideraciones a tomar en cuenta para las figuras donde se muestra el tráfico son:

- Eje horizontal (X): tiempo en segundos de ocupación del canal
- Eje vertical (Y): cantidad de bytes transmitidos

Datos:

Se han realizado varios tipos de pruebas para este análisis:

1) Desde el equipo ubicado en Quito se realiza la transferencia de datos (texto e imágenes), hacia el equipo ubicado en Guayaquil por 30 minutos aproximadamente.

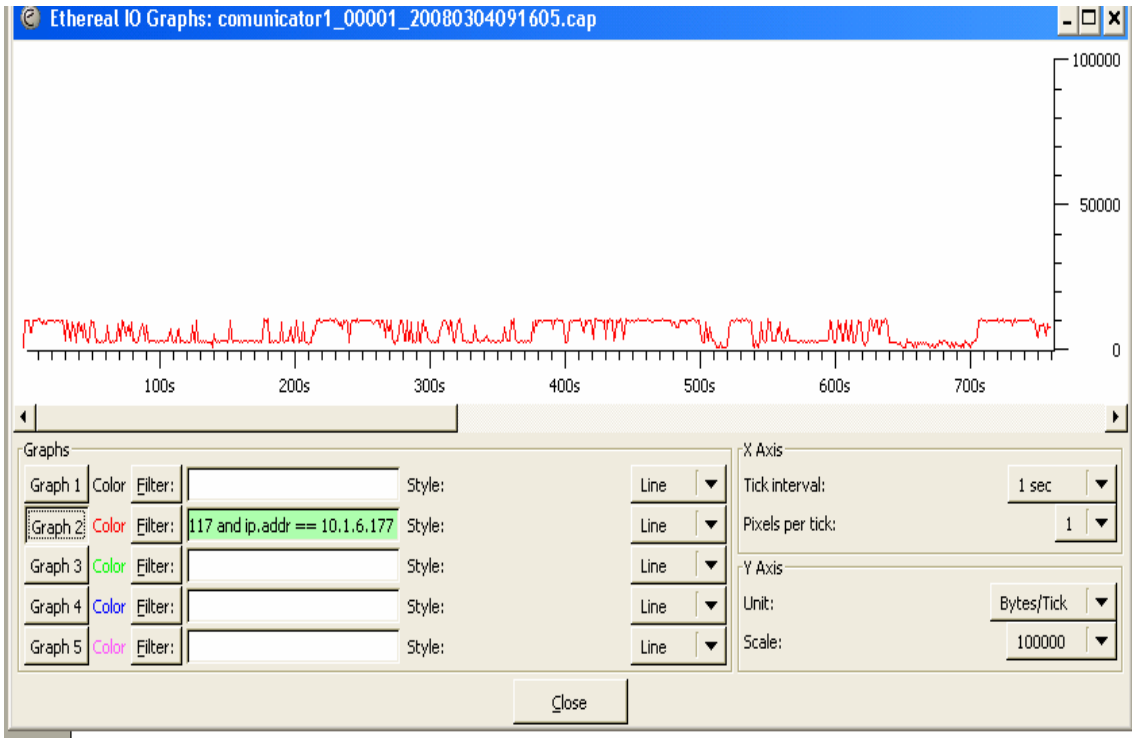


Figura 3.4 Tráfico de datos (texto e imágenes)

En la figura 3.4 se puede observar el consumo de ancho de banda que genera la transmisión de datos, el cual es en promedio 5000 Bytes/segundo, es decir, 40 Kbps.

2) Se accedió a una biblioteca digital ubicada en la Facultad de Medicina de la Universidad Nacional Autónoma de México y se navegó a través de un libro por 7 minutos aproximadamente.

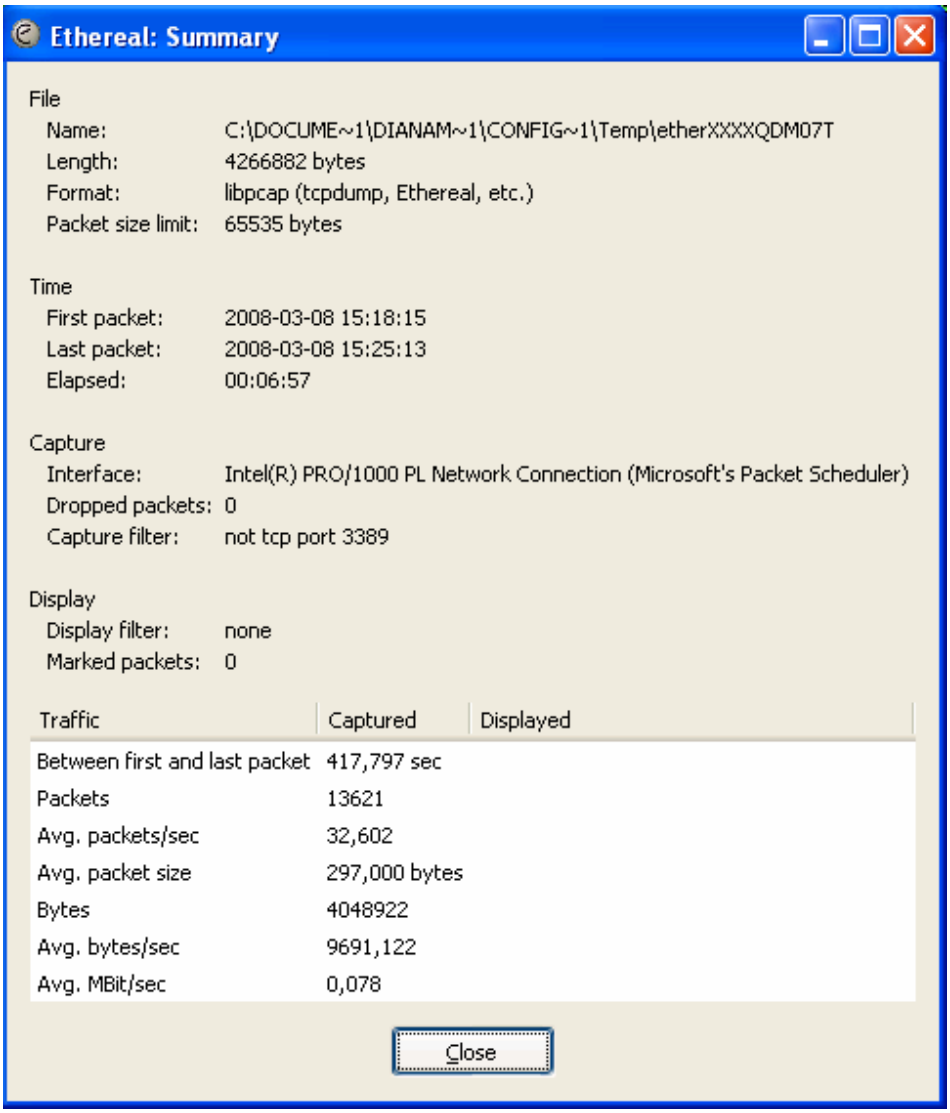


Figura 3.5 Resumen de tráfico por navegación en biblioteca digital

En la figura 3.5 se puede observar un promedio de 9691 Bytes/segundo aproximadamente, transmitidos durante la navegación, es decir, 78 Kbps.

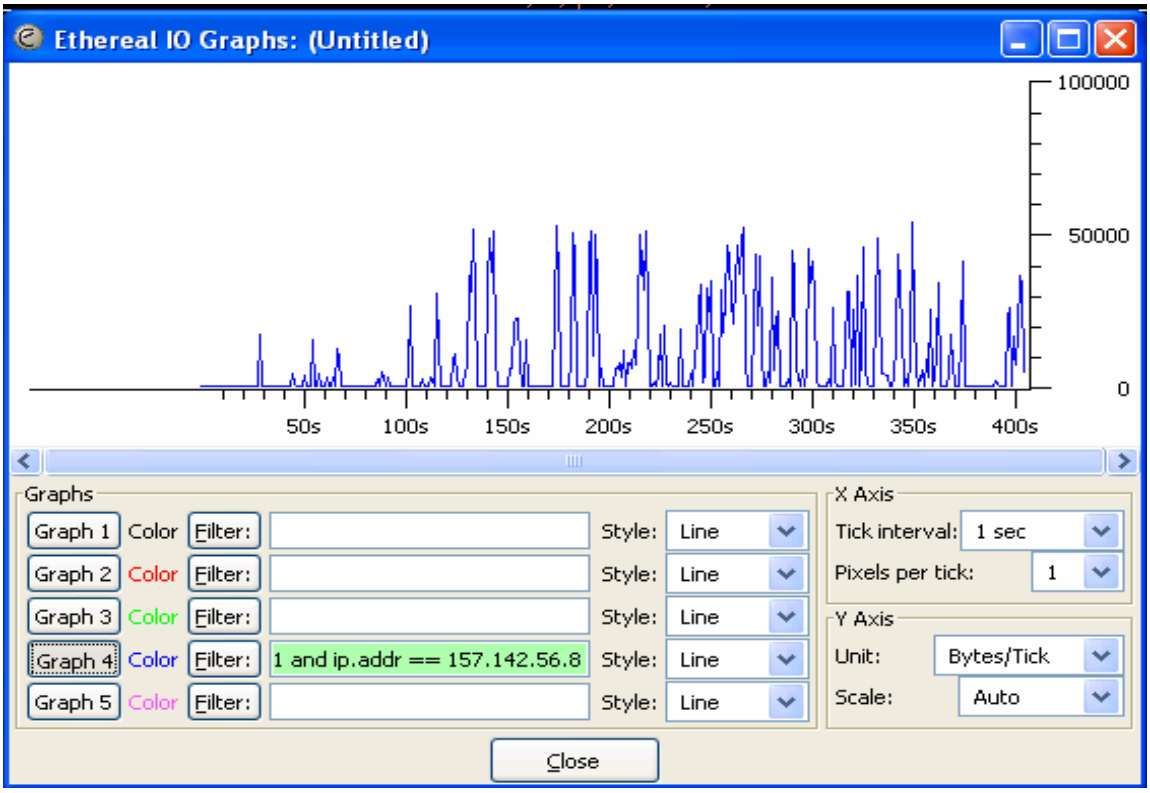


Figura 3.6 Tráfico de datos por navegación en biblioteca digital

3) Se descargó un libro de 3 MB, que es el peso promedio de los libros almacenados en las bibliotecas digitales, de la Universidad Complutense de Madrid. Las figuras 3.7 y 3.8 muestran los resultados obtenidos.

Se puede observar en la figura 3.7, que la velocidad de descarga es de aproximadamente 45046 Bytes/segundo, es decir, 360 Kbps.

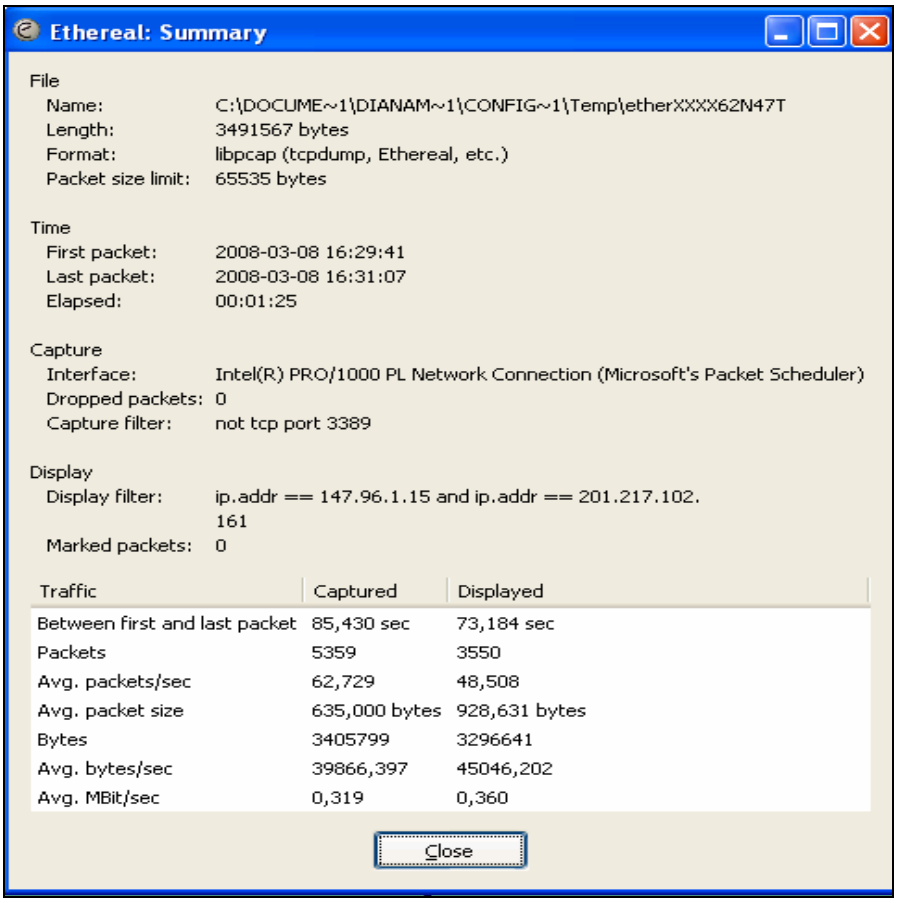


Figura 3.7 Resumen de tráfico de descarga de un libro digital

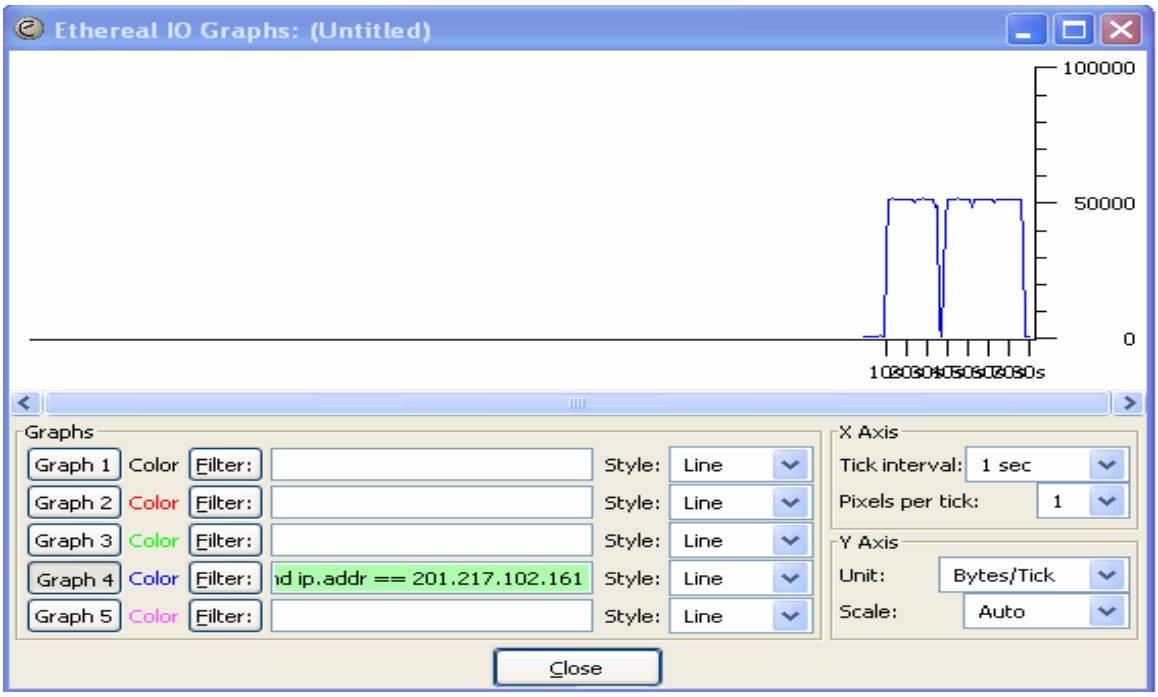


Figura 3.8 Tráfico de datos por descarga de un libro digital

4) Se accedió a un laboratorio virtual, en el que se receptó audio en tiempo real, por aproximadamente 5 minutos. Las figuras 3.9 y 3.10 muestran los datos obtenidos:

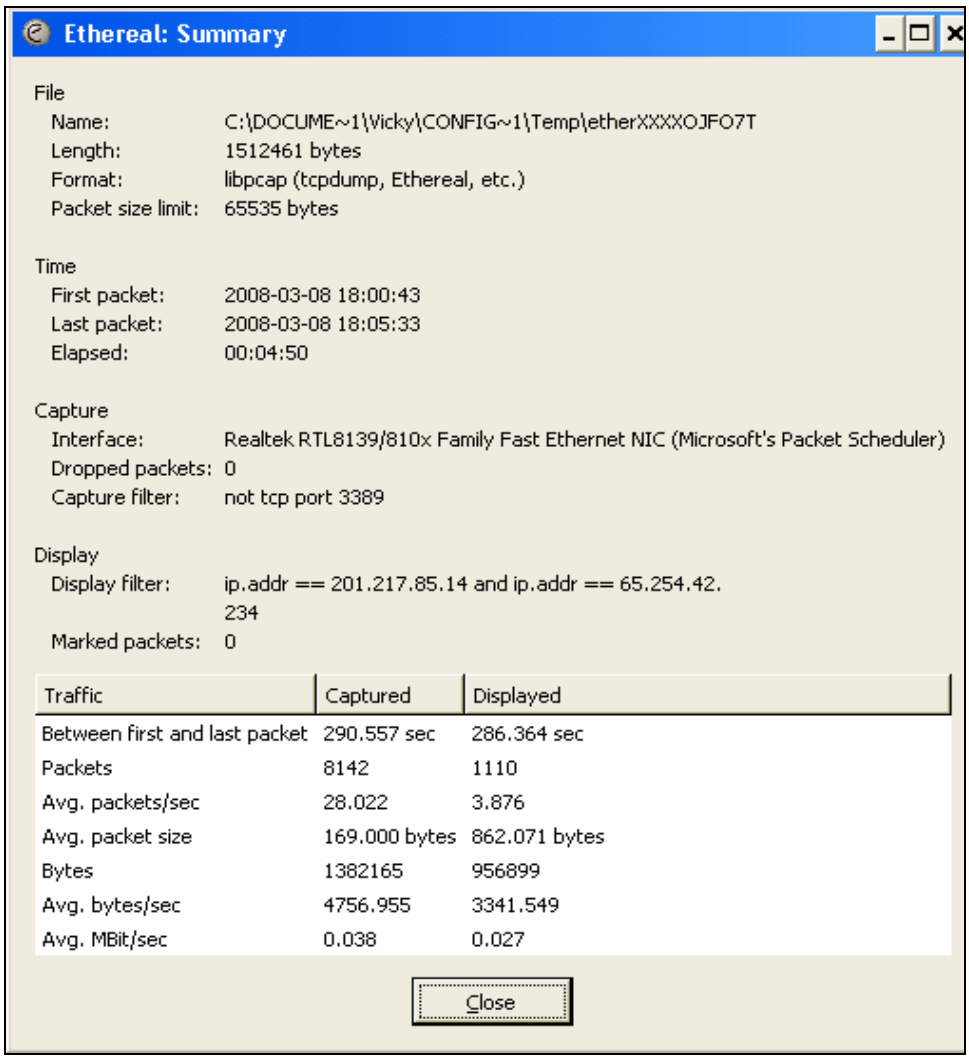


Figura 3.9 Resumen de tráfico de audio en tiempo real

Se puede observar en la figura 3.9 un tráfico promedio de 3341 Bytes/segundo, es decir, 27 Kbps.

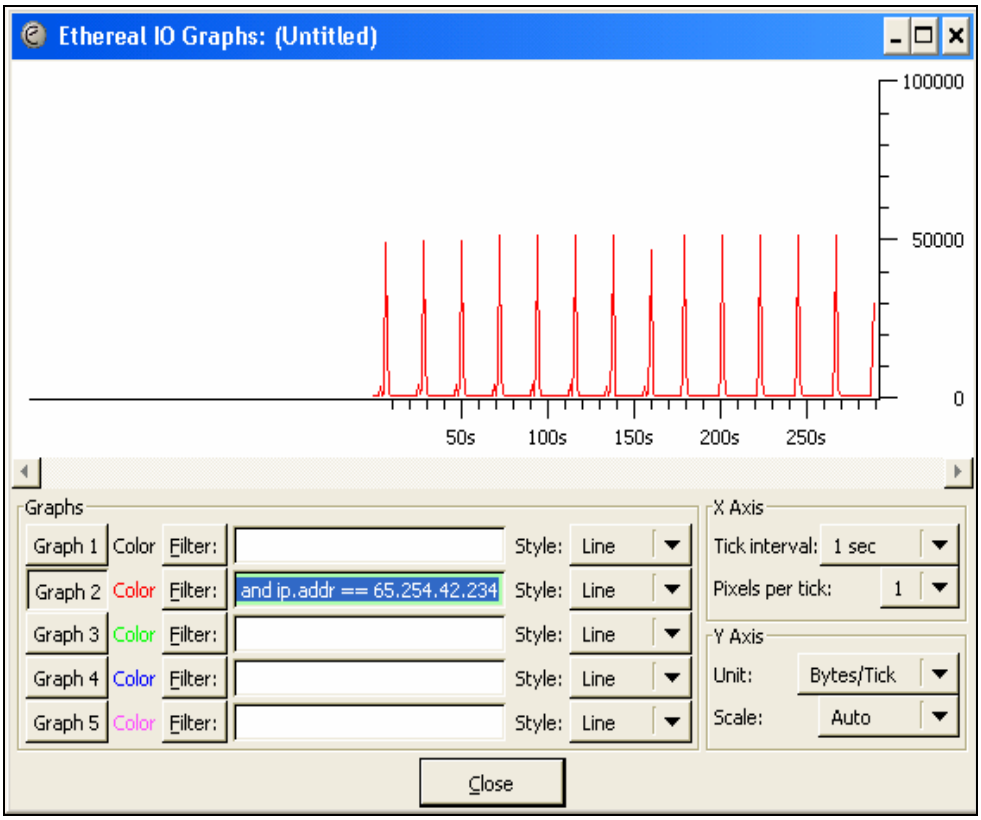


Figura 3.10 Tráfico de audio en tiempo real

5) Se accedió a un laboratorio virtual, del cual se receptó audio y video en tiempo no real, por aproximadamente 7 minutos. En las figuras 3.11 y 3.12 se muestran los resultados obtenidos:

La figura 3.11 nos muestra un tráfico promedio de 7077 Bytes/segundo, es decir, 57 Kbps consumidos.

Se pueden observar en la figura 3.12 picos frecuentes de hasta 50000 Bytes/segundo, es decir, 400 Kbps, valor que variará de acuerdo a la capacidad y al *access rate* del enlace. Cabe mencionar que la duración de cada video es en promedio de 1 minuto.

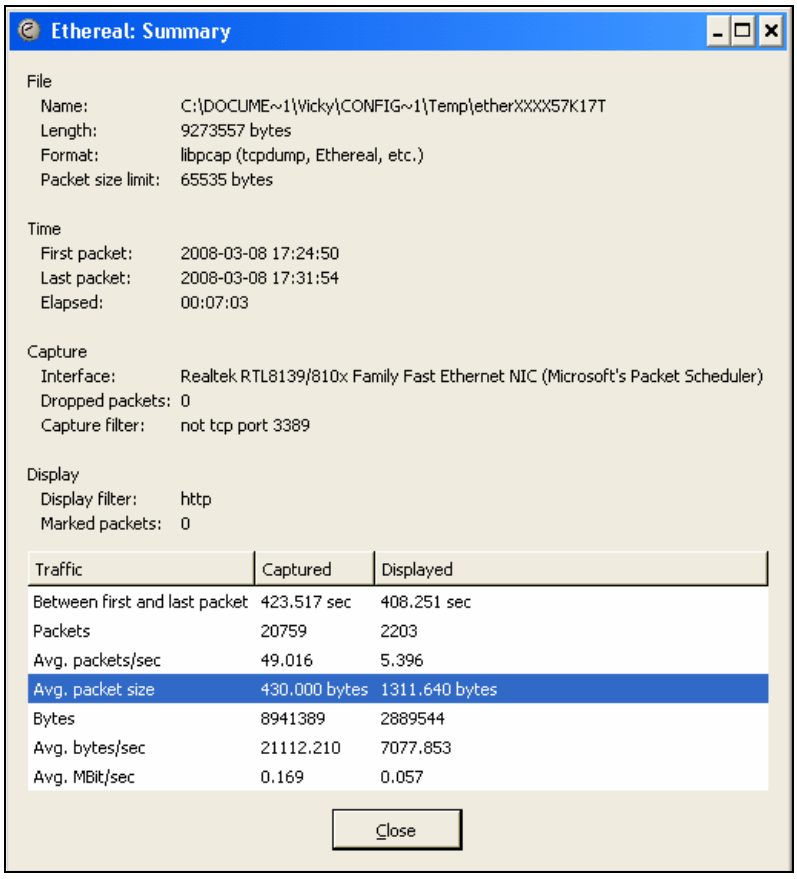


Figura 3.11 Resumen de tráfico de navegación y descarga de videos en un laboratorio virtual

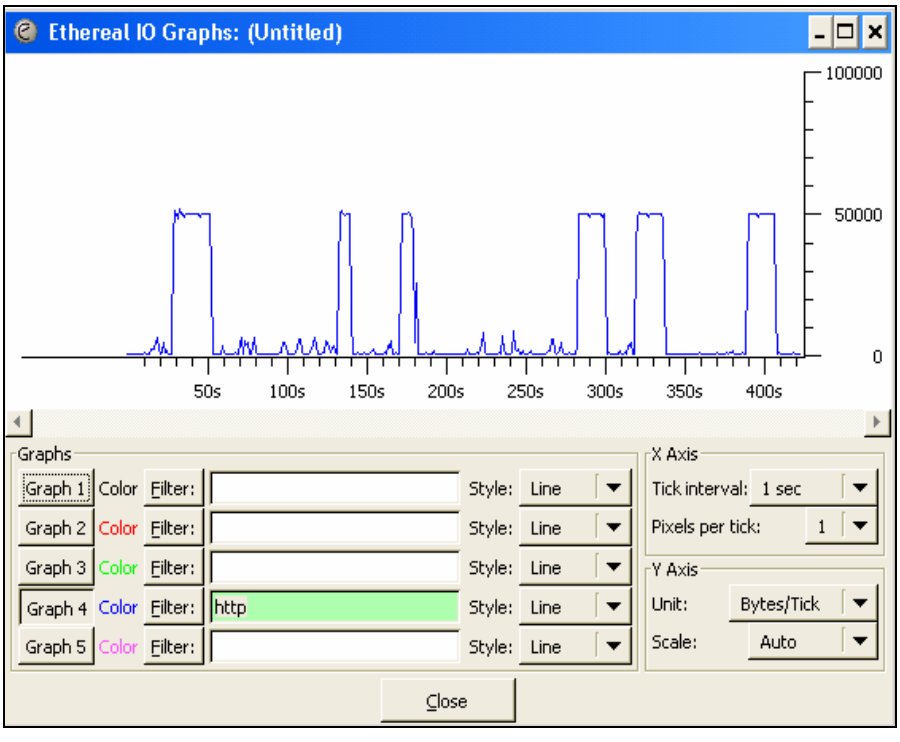


Figura 3.12 Tráfico de navegación y descarga de videos en un laboratorio virtual

Videoconferencia

Se han realizado dos pruebas para el análisis del tráfico generado por la videoconferencia.

1. Se estableció, por media hora aproximadamente, una videoconferencia de calidad baja (0.3 Megapixeles de resolución, alta compresión JPEG) entre un equipo con dirección IP 10.0.5.117 en Quito y un equipo con dirección IP 10.0.150.13 en Guayaquil, mediante la herramienta *Microsoft Office Communicator*.

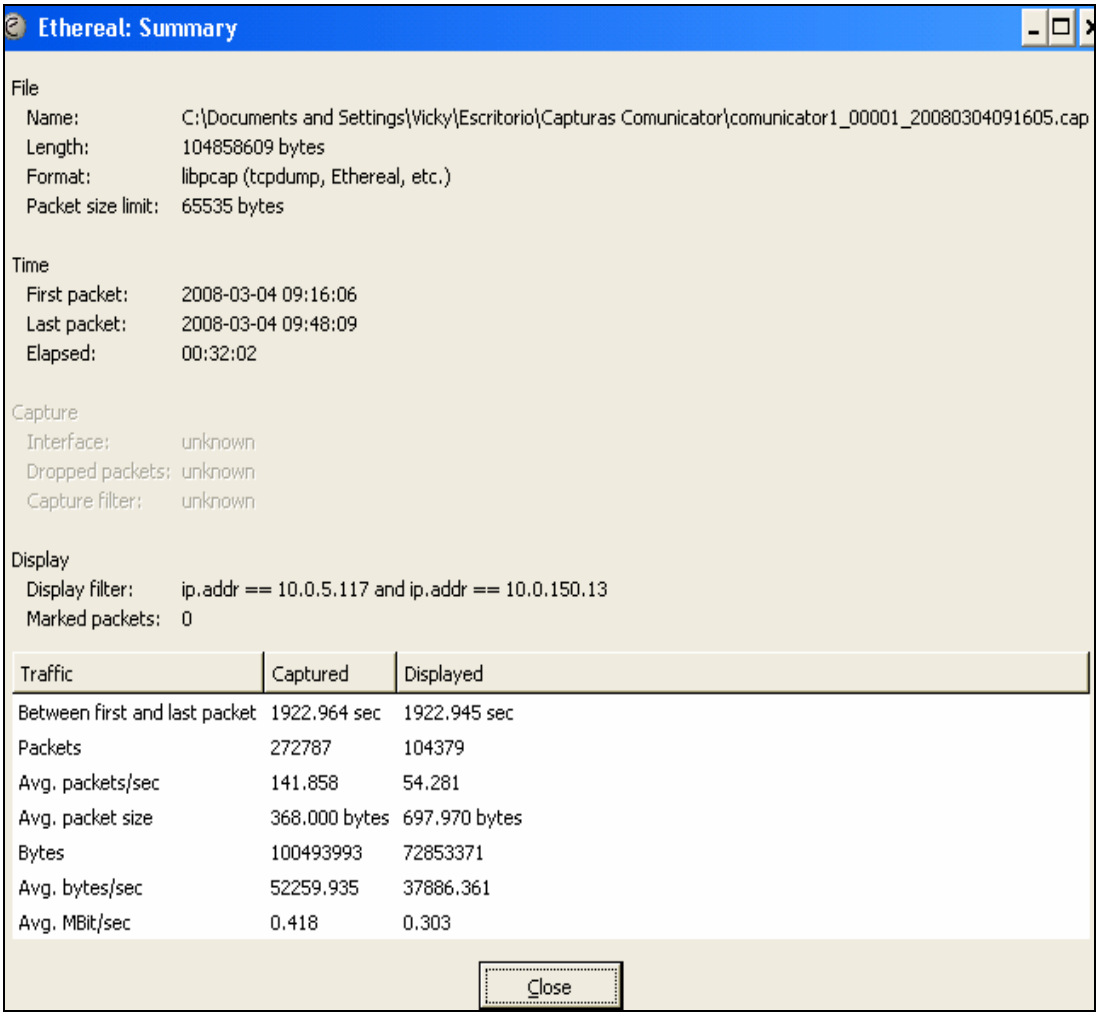


Figura 3.13 Resumen de tráfico de videoconferencia de calidad baja

Como se puede observar en la figura 3.13 existe un promedio de 37886 Bytes/segundo transmitidos aproximadamente, es decir, 303 Kbps.

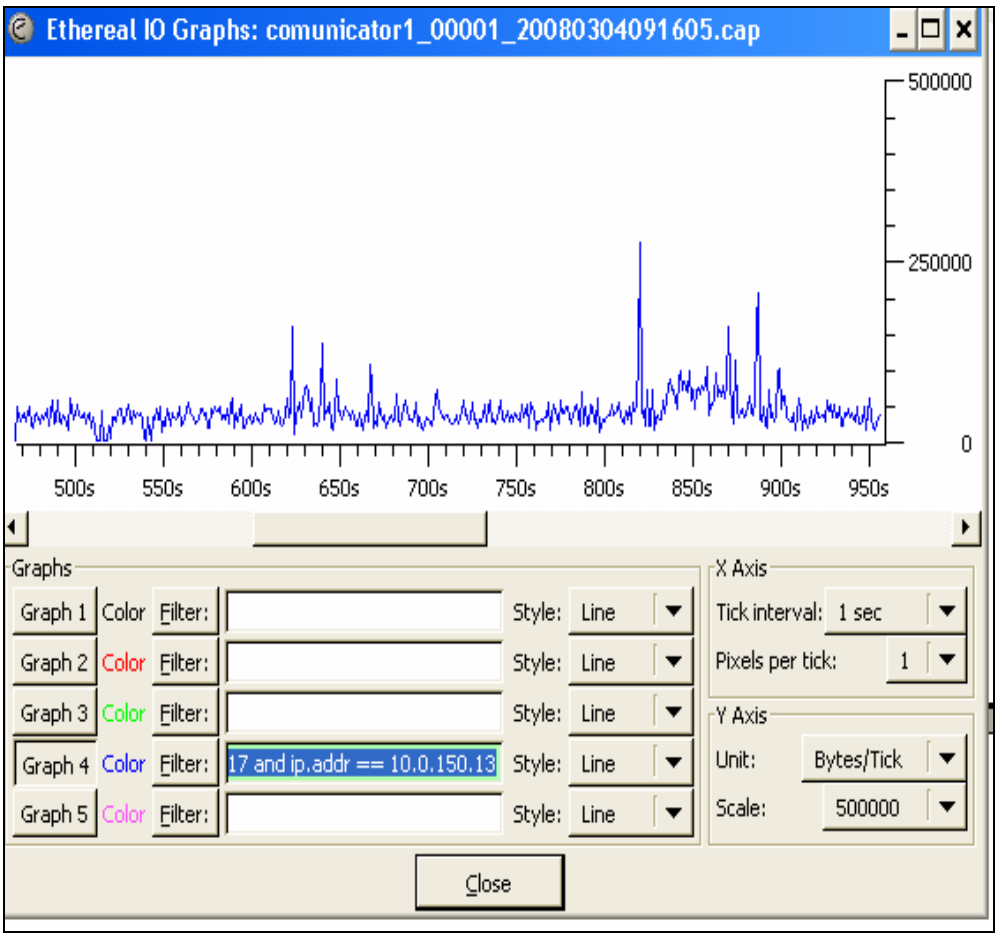


Figura 3.14 Tráfico de datos de videoconferencia de calidad baja

Se observa en la figura 3.14 un pico máximo aproximadamente de 290000 Bytes/segundo, es decir, 2,32 Mbps, sin embargo, los picos que se presentan son esporádicos y no superan los 5 segundos de duración. Por lo anteriormente mencionado no afectan el consumo promedio de la aplicación.

2. Se estableció una videoconferencia de calidad media (1,3 Megapixeles de resolución, baja compresión JPEG) entre el equipo con dirección IP 10.0.5.117 en Quito y un equipo con dirección IP 10.0.150.13 en Guayaquil, mediante la herramienta *Microsoft Office Communicator*.

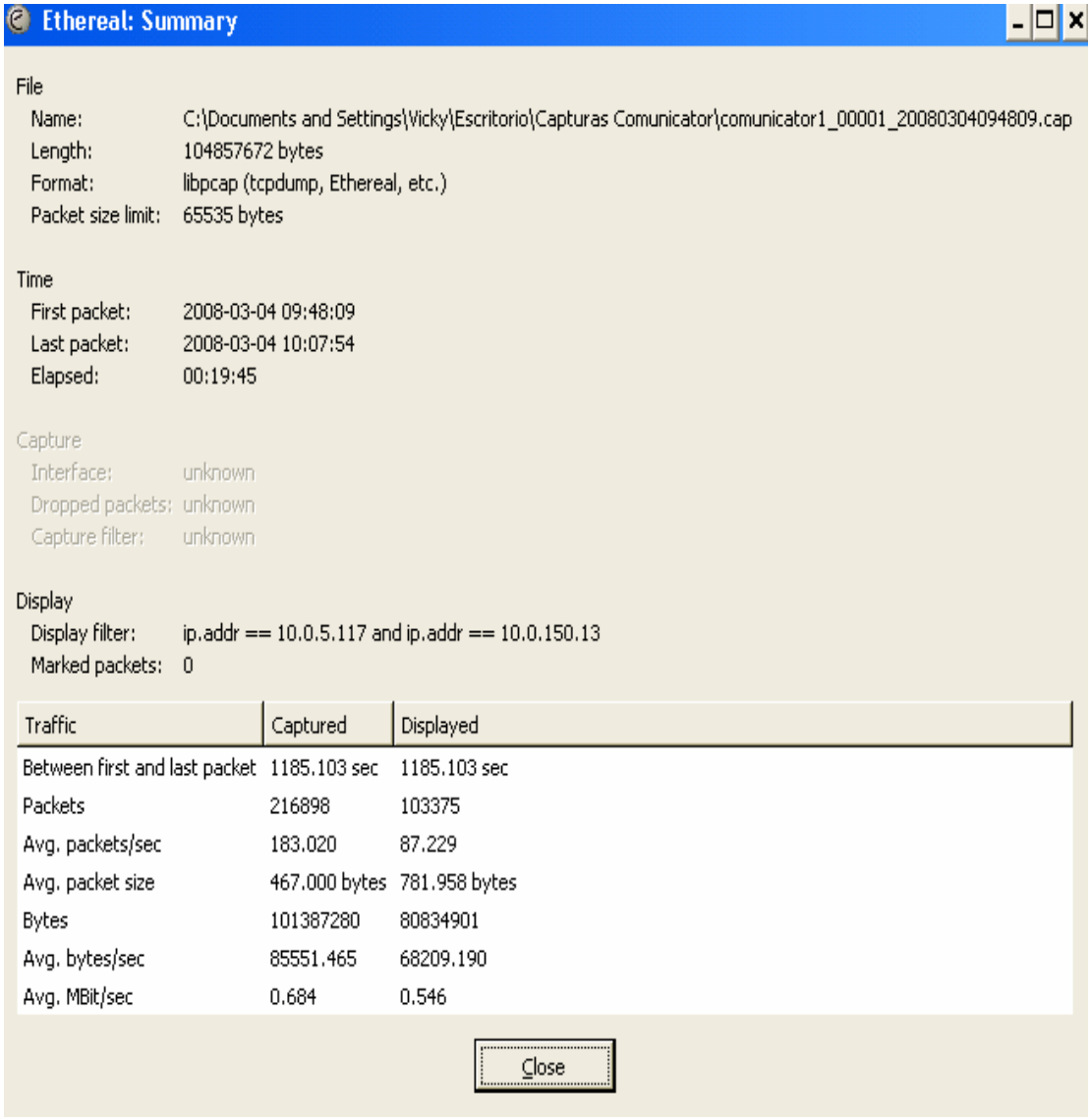


Figura 3.15 Resumen de tráfico de videoconferencia de calidad media

Se puede observar en la figura 3.15 que el promedio del tráfico cursado es de 68209 Bytes/segundo aproximadamente, es decir, 546 Kbps.

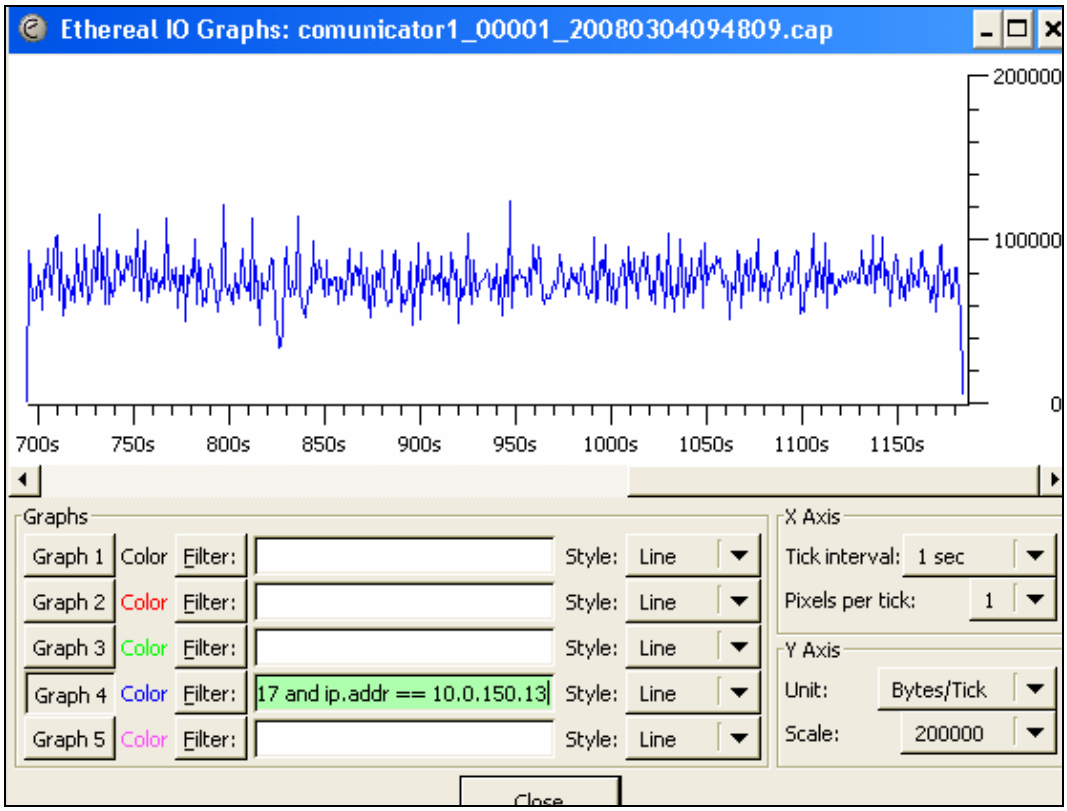


Figura 3.16 Tráfico de datos de videoconferencia de calidad media

Conclusiones del análisis

Cuando se realiza una descarga de un archivo, ya sea éste video, audio, texto o imágenes, se identifica claramente que la descarga tiende a ocupar toda la capacidad del canal. Cabe recalcar que las descargas se las hicieron con dos navegadores Internet Explorer y Mozila Firefox y en ambos casos los resultados fueron similares.

Existen picos de tráfico que superan la capacidad del canal, esto se debe a que el *access rate* es superior a la capacidad contratada. Estas circunstancias se presentan cuando el proveedor del servicio de Internet, permite superar la capacidad contratada cuando el canal está siendo subutilizado por el resto de usuarios que lo comparten.

3.2 ESQUEMA DE FUNCIONAMIENTO DE LOS PROTOCOLOS A UTILIZARSE

Según el estudio realizado en el capítulo 1, la red de CEDIA trabaja con la pila protocolos TCP/IP.

A continuación se mencionarán los protocolos requeridos por las aplicaciones a partir de la capa de transporte del modelo ISO/OSI, debido a que éstos pueden ser utilizados por los usuarios independientemente de la infraestructura de red del proveedor.

En la tabla 3.1 se puede observar los principales protocolos y estándares utilizados por los usuarios en cada una de las aplicaciones.

APLICACIONES	PROTOCOLOS Y ESTÁNDARES
Bibliotecas digitales	HTTP, FTP, DNS, TCP, UDP
Tele-inmersión	RTP, TCP, UDP
Laboratorios virtuales	HTTP, FTP, SCP, RTP, DNS, TCP, UDP
Telemedicina	HTTP, FTP, SCP, TCP, UDP, H.323
VRSV	HTTP, TCP, UDP, H.323
Simulación distribuida	HLA, TCP, UDP
Learningware o *software* de aprendizaje	HTTP, FTP, SCP, DNS, TCP, UDP

Tabla 3.1 Protocolos y estándares utilizados por los usuarios

HTTP (*HyperText Transfer Protocol*) [28]

Protocolo que trabaja a nivel de aplicación, es utilizado por la mayoría de aplicaciones para transmitir información entre el cliente y el servidor de forma clara y rápida.

Se basa en otros estándares como *Uniform Resource Identifier* (URI), *Uniform Resource Location* (URL) y *Uniform Resource Name* (URN), para indicar el recurso al que hace referencia la petición.

FTP (*File Transfer Protocol*) [29]

Protocolo de transferencia de archivos que trabaja a nivel de capa aplicación, utilizado por las aplicaciones para la carga y descarga de archivos a través de la red entre el cliente y el servidor, su principal inconveniente es la transmisión en texto plano.

DNS (*Domain Name System*) [30]

El DNS es una base de datos jerárquica y distribuida que almacena información sobre los nombres de dominio. Es así que llamamos DNS también al protocolo de comunicación entre un cliente y el servidor DNS, el cual ayuda al cliente a resolver nombres de dominio y traducirlos en direcciones IP.

SCP (*Secure Copy Protocol*) [31]

Es un protocolo de transferencia segura de archivos informáticos entre dos computadores, usando el protocolo SSH (*Secure Shell*).

Es utlizado por las aplicaciones que requieren transmisión de información confidencial. Los datos son cifrados durante su transferencia, para evitar que *sniffers* extraigan información de los paquetes de datos. Sin embargo, el protocolo mismo no provee autentificación y seguridad; sino que espera que el protocolo subyacente, SSH, lo asegure.

TCP (*Transmission Control Protocol*) [32]

Se utiliza TCP para crear conexiones entre computadores a través de las cuales se envía un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron.

Este protocolo es vital para la simulación distribuida, laboratorios virtuales y telemedicina, puesto que, estas aplicaciones requieren que los datos transmitidos lleguen en forma correcta a su destino, ya que de éstos depende el resultado de la simulación, del laboratorio o de un correcto diagnóstico.

.

UDP (*User Datagram Protocol*) [33]

UDP es un protocolo a nivel de transporte, basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación, ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o de recepción.

Su uso principal es para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

RTP (*Real-time Transport Protocol*) [34]

Es un protocolo de nivel de transporte cuyo objetivo es brindar un medio uniforme de transmisión sobre IP, de datos que estén sujetos a las limitaciones de tiempo real (audio, voz y video). La función principal de RTP

es implementar los números de secuencia de paquetes IP para rearmar la información de audio, voz o video.

Además, los paquetes de difusión múltiple pueden utilizar RTP para enrutar conversaciones a múltiples destinatarios.

HLA (*High Level Architecture*) [37]

El estándar IEEE-1516 define una arquitectura de alto nivel HLA para simulaciones distribuidas. El objetivo de HLA es permitir la interacción entre simulaciones de una forma sencilla para el programador. Proporciona, en forma de servicios, funcionalidades propias de los entornos de simulación distribuidos, y que no se encuentran implementados en otro tipo de sistemas distribuidos de carácter más general, como por ejemplo servicios específicos de suscripción a eventos o control del tiempo global de simulación.

HLA define los siguientes conceptos asociados a una simulación distribuida:

Federate: Un federado forma con otros una simulación global. Cada federado ejecuta una parte de dicha simulación. Un federado no puede existir nunca por sí solo, siempre debe estar asociado a una federación.

Federation: Una federación es un conjunto de federados que conforman un entorno o una simulación global. Cada federado simula una parte (por ejemplo, la simulación de un avión) dentro de la simulación global (por ejemplo, la simulación del tráfico aéreo de un país).

***RunTime Infraestructure* (RTI):** Proporciona una capa, de abstracción a los federados, que encapsula la problemática adscrita al entorno de simulaciones distribuidas. Un federado se implementa sobre un soporte RTI, que permite la comunicación con otros federados.

H.323 [38]

En el capítulo 2 en la sección 2.2.3 se analizan los estándares utilizados para videoconferencia.

Protocolos utilizados por H.323

A continuación se explican los protocolos más significativos para H.323:

RTP/RTCP (*Real-Time Transport Protocol / Real-Time Transport Control Protocol*): Protocolos de transporte en tiempo real que proporcionan servicios de entrega punto a punto de datos.

RAS (*Registration, Admission and Status*): Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través del *Gatekeeper*.

H.225: Protocolo encargado del control del establecimiento de la llamada: señalización, registro y admisión, y sincronización del flujo de voz.

H.245: Protocolo de administración de la llamada.

Q.931 (*Digital Subscriber Signalling*): Este protocolo se define para la señalización de accesos RDSI básico.

RSVP (*Resource ReSerVation Protocol*): Protocolo de reserva de recursos en la red para cada flujo de información de usuario.

T.120 La recomendación T.120 define un conjunto de protocolos para conferencia de datos

Entre los estándares que recomienda usar la norma H.323 se encuentran principalmente:

G.711: De los múltiples estándares de audio que pueden implementar los terminales H.323, éste es el único obligatorio. Usa modulación por pulsos codificados (PCM) para conseguir tasas de bits de 56 Kbps y 64 Kbps.

H.261y H.263: Son los dos estándares de video que propone la recomendación H.323. Sin embargo, se pueden usar otros.

El estándar H.261 fue diseñado para una tasa múltiplo de 64 Kbps, utiliza *buffers* para moderar las variaciones en la tasa de emisión de bits del codificador de vídeo. Se puede conseguir una tasa de emisión de bits casi constante realimentando el estado del *buffer* al codificador.

El objetivo para H.263 era proporcionar mejor calidad de imagen que el algoritmo de compresión de vídeo de ITU-T existente, H.261, pero todavía no se ha logrado. El H.263, además de utilizar nuevas técnicas de codificación, emplea técnicas conocidas como la transformada coseno discreta y la compensación de movimiento.

3.3 CÁLCULO DE LAS CAPACIDADES DE LOS ENLACES

Para el dimensionamiento de las capacidades que requieran cada una de las aplicaciones de las redes avanzadas, se tomarán en cuenta varios factores, entre ellos:

- Análisis de tráfico realizado en la sección 3.1.
- Número de usuarios.
- Factor de concurrencia (simultaneidad).
- Tiempo estimado en descargas.
- Valor promedio de *Bytes* a descargar.
- *Overhead*.
- Políticas de utilización de las aplicaciones.

En este caso, se asumirá un número de usuarios (N) que estén usando determinada aplicación, de estos usuarios con una proporción del Factor de Concurrencia (Fc) se calculará el número de clientes realizando ciertas actividades (Nc).

Con los datos de la sección 3.1 se realizará el cálculo de la capacidad necesaria para que los usuarios accedan a las aplicaciones.

Se realizará el dimensionamiento para cada una de las aplicaciones y al final se establecerán las políticas para optimización del uso del canal.

3.3.1 BIBLIOTECAS DIGITALES

A través de una biblioteca digital se pueden realizar varias actividades, entre las cuales se destacan:

- Navegación a través de libros, revistas, folletos, entre otros.
- Descarga de libros, revistas, folletos, etc.
- Descarga de audio y video en tiempo no real.

Para cada una de estas actividades se realizará el cálculo de la capacidad necesaria para su correcta ejecución.

Primeramente, se debe resaltar el hecho de que en la actualidad la red avanzada ecuatoriana se encuentra sub-utilizada, por lo que, el número de usuarios a asumirse será pequeño.

Se asumirán 10 usuarios accediendo a la biblioteca digital.

Navegación

Cuando un usuario accede a un libro, revista u otro documento de la biblioteca digital, requiere de un ancho de banda en promedio de 78 Kbps, según el análisis de tráfico realizado en la sección 3.1.

Por lo tanto:

N = 10

AB = 78 Kbps

Si los 10 usuarios, se encuentran al mismo tiempo navegando a través de la biblioteca digital, la capacidad requerida sería de:

N * AB = 10 * 78 Kbps = 780 Kbps

Descargas

Se realizará el cálculo primeramente para el caso, de que la descarga sea de un libro ya que es la actividad más frecuente.

Los documentos de texto e imágenes dentro de una biblioteca digital son almacenados en varios formatos .doc .pdf, etc. El más común y de mayor utilización es el formato PDF. PDF (*Portable Document Format*) es un formato muy interesante para crear *e-books*. Tiene una buena compresión lo que hace que se pueda ver el texto de una forma muy estética a la vez que ocupa poco espacio.

Además es importante tomar en cuenta aspectos de seguridad, tales como, el no permitir su reproducción y distribución ilícita, ya que la información es de libre acceso para todo el mundo; este formato ha sido adoptado por las bibliotecas digitales en su gran mayoría.

Sin embargo no se puede establecer un valor exacto en *bytes* del tamaño de un libro ya que éste depende de algunas variables, como por ejemplo:

- Número de páginas.
- Número de imágenes que contenga.
- Compresión utilizada en el momento de la construcción, etc.

Es así que dos libros con igual número de páginas podrían tener tamaños diferentes, por la simple razón que el momento que el libro fue creado, un constructor utilizó una tasa de compresión menor que el otro.

Ahora al tratarse de información que no es crítica, es decir, no es transmitida en tiempo real se pueden establecer tiempos de descarga aceptables para el usuario, por ejemplo:

Un texto de aproximadamente 150 hojas en formato pdf con imágenes de calidad media pesa alrededor de 3 MB, lo cual, se considera aceptable descargarlo en 2 minutos a través de una red avanzada, lo que da como requerimiento obtener una velocidad de transmisión de:

$$\frac{3MBytes}{2\min} * \frac{8bits}{1Byte} * \frac{1\min}{60s} = 200Kbps$$

Este valor, 200 Kbps, está calculado para un solo usuario y sin tomar en cuenta el *overhead*.

Con los valores obtenidos en el análisis de tráfico podemos calcular un valor estimado de *overhead*.

Un archivo de 3 MB fue descargado en 73 segundos con una tasa de transferencia de 360 Kbps en promedio.

$$360Kbps * 73s * \frac{1byte}{8bits} = 3.285MB$$

Del resultado obtenido se puede concluir que para descargar un archivo de 3 MB se necesitarán 285 KB adicionales que representan el *overhead*.

$$\%overhead = \left[\frac{3.285}{3} - 1 \right] * 100\% = 9.5\%$$

Por lo tanto, el valor requerido para descargar un libro de 3 MB en 2 min será:

200 Kbps * 1.095 = 219 Kbps

Basándose en el número de usuarios asumidos N = 10 y en el factor de concurrencia Fc = 10%, valor tomado como referencia de un proyecto del Departamento de Señales de de la Universidad Politécnica de Madrid y de una tesis doctoral de la Universidad de la Salle de Bogotá. [83] [84].

Ncd = N*Fc = 10 * 0.1 = 1 usuario

De los 10 usuarios, uno de ellos estará descargando algún documento de texto e imágenes.

Por lo tanto, la capacidad del canal requerida sería:

(N – Ncd) * 78 Kbps + Ncd * 219 Kbps = (10-1)*78 Kbps + 1*219 Kbps = 921 Kbps

En el caso de que la descarga sea de audio y video en tiempo no real, de un documental por ejemplo, se tomarán en cuenta valores correspondientes a este tipo de información.

Un video de calidad media, de tiempo promedio de duración de 1 minuto, con compresión MPEG, pesa alrededor de 4.5 Mbps.

Se considera un tiempo de descarga aceptable de 2 minutos, por lo tanto, la capacidad requerida para un usuario sería igual a:

$$\frac{4.5MBytes}{2\min} * \frac{8bits}{1Byte} * \frac{1\min}{60s} = 300Kbps$$

Considerando el *overhead* calculado anteriormente se tiene:

300 Kbps * 1.095 = 328.5 Kbps

Con los datos anteriores de N y Fc, se calculará el número de usuarios que están descargando video y audio en tiempo no real simultáneamente Ncv:

Ncv = N*Fc = 10 * 0.1 = 1 usuario

Por lo tanto, considerando que de los 10 usuarios, uno estará descargando un documento con texto e imágenes y otro estará descargando audio y video en tiempo no real, la capacidad requerida para 10 usuarios accediendo a una biblioteca digital, sería:

(N - Ncd - Ncv) * 78 Kbps + Ncd * 219 Kbps + Ncv * 328.5 Kbps = (10-1-1)*78 Kbps + 1*219 Kbps + 1*328.5 Kbps = 1171.5 Kbps

3.3.2 TELEINMERSIÓN

En la actualidad no es factible la implementación de esta aplicación en la red avanzada ecuatoriana, pero, se mencionará un valor aproximado de la capacidad requerida para su ejecución, en base a estudios realizados por redes que si la soportan.

Para el respectivo cálculo, se debe utilizar la siguiente ecuación:

Data Rate Per Participant Site = Resolution por Frame * Bits por Pixel * Frames por Segundo * Data Compression Ratio*Número de vistas para reconstrucción.

Ecuación 1 Tráfico en tele-inmersión [11]

Una prueba realizada por *University of North Carolina at Chapel Hill*, utilizó los siguientes valores: [11]

Resolution por *Frame*	320*240 [pixels/frame]
Bits por Píxel	40
Frames por Segundo	30
Data Compression Ratio	1/6
Número de vistas para reconstrucción	5
Data Rate	**76800000 [bits/segundo]**

Se puede comprobar el valor obtenido, reemplazando los valores en la ecuación:

Data Rate Per Participant Site = 320*240 * 40 * 30 * 1/6 *5 = 76800000 bps = 76.8 Mbps

Se puede concluir que, para que un solo usuario utilice teleinmersión se necesita una capacidad de 76,8 Mbps, valor que se encuentra muy lejano de las capacidades contratadas por los miembros para el acceso a la red avanzada ecuatoriana.

3.3.3 LABORATORIOS VIRTUALES

De acuerdo al estudio realizado en el capítulo 2 se pueden identificar varios tipos de laboratorios, que iban desde un nivel inferior con la manipulación de imágenes en 2D, hasta un nivel en el que se podría utilizar la tele-inmersión como aplicación para desarrollar el laboratorio.

Si bien, este último es un avance realmente revolucionario en el mundo de las comunicaciones, en la práctica aún se encuentra en desarrollo, debido a que los requerimientos son demasiado elevados como por ejemplo:

- Sentir objetos remotos.

Para esto la ciencia está desarrollando dispositivos capaces de captar olores, texturas y poder transmitirlas.

En un laboratorio virtual se han identificado las siguientes principales actividades:

- Navegación a través de un laboratorio virtual
- Receptar audio en tiempo real
- Descarga de audio y video en tiempo no real.

Se asumirán un número de usuarios del laboratorio virtual N = 10.

Navegación a través de un laboratorio virtual

Si los usuarios se encuentran únicamente navegando a través de un laboratorio virtual, realizando actividades que no requieren muchos recursos de la red, por ejemplo manipulación de texto e imágenes en 2D, el

ancho de banda consumido por un usuario es de 78 Kbps según el análisis de tráfico realizado en la sección 3.1.

La capacidad requerida para los 10 usuarios sería:

$$N * AB = 10 * 78 \text{ Kbps} = 780 \text{ Kbps}$$

Recepción de audio en tiempo real

En base al análisis de tráfico realizado en la sección 3.1, la transmisión de audio de calidad aceptable requiere aproximadamente de 27 Kbps por usuario.

Considerando un factor de concurrencia igual a Fc = 10%, el número de usuarios realizando esta actividad sería:

$$Nca = N*Fc = 10 * 0.1 = 1 \text{ usuario}$$

Por lo tanto, para los 10 usuarios, la capacidad requerida es:

$$(N - Nca) * 78 \text{ Kbps} + Nca * 27 \text{ Kbps} = (10-1)*78 \text{ Kbps} + 1*27 \text{ Kbps} = 729 \text{ Kbps}$$

Descarga de video y audio

De acuerdo al cálculo realizado para la aplicación bibliotecas digitales la capacidad requerida para la descarga de un video que incluye audio es 328.5 Kbps para un usuario.

Considerando un factor de concurrencia del 10%, el número de usuarios descargando video y audio (Ncv) es:

$$Ncv = N*Fcv = 10 * 0.1 = 1 \text{ usuario}$$

La capacidad requerida para que 10 usuarios accedan a un laboratorio virtual es:

(N - Nca - Ncv) * 78 Kbps + Nca * 27 Kbps + Ncv * 328.5 Kbps = (10-1-1)*78 Kbps + 1*27 Kbps + 1*328.5 Kbps = 979.5 Kbps

3.3.4 TELEMEDICINA

De acuerdo al estudio realizado en el capítulo 2 se tienen las principales aplicaciones de Telemedicina:

- Telediagnósis.
- Teleconsulta.
- Reuniones médicas para obtener segundas opiniones.
- Almacenamiento digital de datos o fichas médicas.

La telediagnósis, teleconsulta y reuniones médicas requieren la transmisión de imágenes de alta calidad por la red y videoconferencia, el almacenamiento digital de datos se lo realiza en servidores de bases de datos.

Al ser la telemedicina una aplicación muy importante, la videoconferencia debe ser al menos de calidad media y la transmisión de imágenes debe realizarse en un bajo tiempo.

Telediagnósis, Teleconsulta y Reuniones Médicas [25]

En estas aplicaciones se requiere establecer una videoconferencia y a más de eso la transmisión de elementos digitales como radiografías, mamografías, etc.

La codificación mediante JPEG a tasas de compresión altas produce "artefatos". Éstos son alteraciones en la imagen, son píxeles que en principio no estaban y que aparecen después de realizada la compresión. Los artefatos pueden llegar a ser un grave problema el momento de un diagnóstico ya que el especialista puede leer mal la imagen y producir resultados equívocos.

Por este motivo se recomienda que la compresión sea máxima de 10:1.

A continuación se muestra una tabla, en la que se puede observar el tiempo de transmisión de una imagen con determinado ancho de banda del canal.

ANCHO DE BANDA [Kbps]	**256**	**512**	**1024**	**2048**
Radiografía Digital [s]	5	2,5	1,25	0,625
Mamografía [s]	2,622	1,311	0,6555	0,32775
Radiografía Computarizada [s]	1,25	0,625	0,3125	0,15625
Angiografía [s]	1,092	0,546	0,273	0,1365
Resonancia Magnética [s]	1,024	0,512	0,256	0,128
Tomografía Computarizada [s]	0,614	0,307	0,1535	0,07675
Ultrasonido [s]	0,492	0,246	0,123	0,0615
Medicina Nuclear [s]	0,042	0,021	0,0105	0,00525

Tabla 3.2 Tiempos de transmisión para diferentes anchos de banda con compresión [26]

Se considerará para el cálculo un número de usuarios igual a N = 10.

Primeramente, se calculará la capacidad requerida para establecer una videoconferencia de calidad media.

Según el análisis realizado en la sección 3.1, una videoconferencia de calidad media requiere un ancho de banda de aproximadamente 546 Kbps. Tomando como referencia el factor de concurrencia recomendado por Microsoft, el cual manifiesta que de 50000 usuarios deberán existir 7500 usuarios simultáneos, es decir, Fcv = 15 %, se calculará el número de usuarios estableciendo una videoconferencia simultáneamente: [24]

$$Ncv = N*Fcv = 10 * 0.15 = 1.5 \approx 2 \text{ usuarios}$$

Para el almacenamiento digital de datos se tomará como referencia el ancho de banda obtenido en el análisis de tráfico de transmisión de datos de la sección 3.1, AB = 40 Kbps.

Se considerará como caso especial la transmisión de imágenes, debido a su gran importancia en la telemedicina. Se tomará como referencia la capacidad de 256 Kbps de los valores recomendados en la tabla 3.1, para asegurar los tiempos de transmisión requeridos. Se asumirá un factor de concurrencia igual al de la videoconferencia, debido a que este tipo de información se transmite con gran frecuencia en esta aplicación.

Por lo tanto, el número de usuarios , que transmiten simultáneamente imágenes (Nci) es:

$$Nci = N*Fci = 10 * 0.15 = 1.5 \approx 2 \text{ usuarios}$$

Se asumirá que, si un usuario no se encuentra en una videoconferencia o no se encuentra transmitiendo imágenes, está transmitiendo datos.

La capacidad requerida para la telemedicina, con un número de usuarios igual a 10, es:

(N - Ncv - Nci) * 40 Kbps + Ncv * 546 Kbps + Nci * 256 Kbps = (10-2-2)*40 Kbps + 2*546 Kbps + 2*256 Kbps = 1844 Kbps

3.3.5 VRSV

El sistema de videoconferencia basado en salas virtuales permite conectarse con varias personas al mismo tiempo sin importar la ubicación geográfica de las mismas.

Las principales actividades realizadas en un VRSV, son:

- Establecimiento de una videoconferencia
- Transmisión de datos

Se asumirá un número de usuarios igual a N = 10.

No se considera necesario el establecimiento de una videoconferencia de calidad, por lo que, se tomará como referencia el valor obtenido en el análisis de tráfico de la sección 3.1, el cual es aproximadamente 303 Kbps.

Debido al uso de *multicast* en la red avanzada ecuatoriana, la capacidad de 303 Kbps se mantendrá constante, así n usuarios estén accediendo a la misma videoconferencia, por lo que, se asumirá el factor de concurrencia recomendado

por Microsoft, para calcular el número de usuarios que estarían accediendo a distintas videoconferencias Fcv=15%.

$$Ncv = N*Fcv = 10 * 0.15 = 1.5 \approx 2 \text{ usuarios}$$

En la transmisión de datos se tomará como referencia el valor obtenido en el análisis de tráfico de datos de la sección 3.1, el cual es aproximadamente 40 Kbps. Se asumirá un factor de concurrencia igual a Fcd = 10%.

$$Ncd = N*Fcd = 10 * 0.10 = 1 \text{ usuario}$$

Es necesario recalcar, que un usuario que accede a un VRSV, lo hace con el fin de participar en una videoconferencia, por lo que, en menor porcentaje existirán usuarios transmitiendo datos.

La capacidad requerida para que 10 usuarios accedan a los VRSVs es:

303 Kbps + Nv * 303 Kbps + Nd*40 Kbps = 303 Kbps + 2*303 Kbps + 1*40 Kbps = 949 Kbps

3.3.6 SIMULACIÓN DISTRIBUIDA

En la simulación distribuida se requiere la transmisión de datos a través de la red.

Está basada en ciertos estándares descritos en el capítulo anterior, los cuales consideran aceptable una velocidad de transmisión de 30 Kbps por cada simulador.

En el análisis de tráfico de datos de la sección 3.1, se obtuvo aproximadamente un valor de 40 Kbps requerido para la transmisión de datos , el cual, cumple con los estándares, por lo tanto, se tomará como referencia.

Se asumirá un número de usuarios igual a N = 10.

La capacidad requerida para que 10 usuarios utilicen simulación distribuida, con la ayuda de un solo simulador, es:

N*40 Kbps = 10*40 Kbps = 400 Kbps

3.3.7 *LEARNINGWARE* O *SOFTWARE* DE APRENDIZAJE

Un sistema de aprendizaje a distancia debe contener todo el material didáctico posible que garantice la correcta enseñanza a sus usuarios.

El estudiante o usuario interactúa con el sistema de tal forma que la información que le proporciona es el material de aprendizaje que debe asimilar.

Dependiendo de cual sea el tópico de la clase, la información variará. Sin embargo se distingue claramente que este sistema transferirá:

- Datos
- Video y audio en tiempo no real

Todos estos datos se deben procurar transmitir en el menor tiempo posible de manera que exista una interacción del usuario con el sistema casi de manera automática.

Se considerará un número de usuarios igual a 10.

Datos

Se tomará como referencia el valor de 40 Kbps obtenido en el análisis de tráfico de datos de la sección 3.1.

Video y audio en tiempo no real

De acuerdo al cálculo realizado anteriormente, la capacidad requerida para la descarga de un video que incluye audio es 328.5 Kbps para un usuario.

Considerando un factor de concurrencia del 10%, el número de usuarios descargando video y audio es:

Ncv = N*Fcv = 10 * 0.1 = 1 usuario

La capacidad requerida para que 10 usuarios utilicen *software* de aprendizaje es:

(N - Ncv) * 40 Kbps + Ncv * 328.5 Kbps = (10-1)*40 Kbps + 1*328.5 Kbps = 688.5 Kbps

Hasta este momento no se ha considerado el *overhead* generado por el protocolo IPv6, a continuación se mencionará un valor estimado.

Se debe tomar en cuenta que el protocolo IPv6 añade una cabecera de 40 bytes al paquete de datos. Por lo tanto, si se toma como referencia el tamaño promedio de los paquetes del análisis de tráfico realizado en la sección 3.1 y se les añade 40 bytes correspondientes a la cabecera del protocolo IPv6, se obtiene un valor aproximado de *overhead*.

Tráfico	Tamaño promedio de paquete [bytes]	Tamaño de paquete sumado 40 bytes [bytes]
Navegación	297	337
Descarga de libro	928	968
Audio tiempo real	862	902
Descarga de video y audio en tiempo no real	1311	1351
Videoconferencia calidad media	698	738
Videconferencia calidad alta	781	821
Promedio	**812.83**	**852.83**

Tabla 3.3 Tamaños promedios de paquetes

$$Overhead = \left(\frac{852.83}{812.83} - 1\right) * 100\% = 4.92\%$$

Este valor obtenido, es un porcentaje estimado, que nos sirve de referencia para obtener un valor más aproximado del consumo de ancho de banda que requiere cada aplicación.

El porcentaje de *overhead* 4.69 % será añadido a los valores calculados en el dimensionamiento de las capacidades requeridas por cada una de las aplicaciones.

APLICACIONES	CAPACIDAD [Mbps]	CAPACIDAD + 4.92% [Mbps]
Bibliotecas digitales	1.180	1.238
Tele-inmersión	76.8	80.578
Laboratorios virtuales	0.98	1.028
Telemedicina	1.844	1.935
VRSV	0.949	0.996
Simulación distribuida	0.400	0.42
Learningware o software de aprendizaje	0.689	0.723

Tabla 3.4 Cálculo de la capacidad considerando *overhead* IPv6

Se resumirá en una tabla, los valores obtenidos a partir del cálculo para 10 usuarios de cada aplicación, a excepción de la Teleinmersión.

APLICACIONES	CAPACIDAD REQUERIDA [Mbps]
Bibliotecas digitales	1.238
Tele-inmersión	80.578
Laboratorios virtuales	1.028
Telemedicina	1.935
VRSV	0.996
Simulación distribuida	0.42
Learningware o software de aprendizaje	0.723

Tabla 3.5 Capacidades requeridas por las aplicaciones

Políticas de utilización

Como se puede observar en la tabla 3.5, la mayoría de aplicaciones requiere una capacidad alrededor de 1 Mbps, a excepción de la Telemedicina que requiere aproximadamente 2 Mbps y la Teleinmersión cuyo valor se ha mencionado únicamente como referencia.

Como se mencionó en el capítulo 1, un miembro de CEDIA posee como mínimo una capacidad contratada de 1 Mbps, por lo que, en caso de estar limitados a esta capacidad, se deberá disminuir el número de usuarios a utilizar cada aplicación.

Para optimizar el uso del enlace y garantizar el correcto funcionamiento de cada una de las aplicaciones, se plantean las siguientes políticas de utilización para un miembro tipo de CEDIA.

1. El número de usuarios por cada aplicación no deberá sobrepasar el valor de 10.

2. Se podrá acceder a dos aplicaciones al mismo tiempo, a excepción de la Telemedicina, que no deberá combinarse con alguna otra aplicación durante su ejecución.

3. Se podrá utilizar la telemedicina a partir de las 17:00 hasta las 19:00, horario en el cual, las demás aplicaciones no deberán ser ejecutadas.

Se sugiere los siguientes horarios, los mismos que pueden ser adaptados según las necesidades e intereses del miembro:

4. Los días Lunes se accederá a las aplicaciones en el siguiente horario:

7:00 a 9:00 → Bibliotecas Digitales – □omerse□ísti Virtuales

9:00 a 11:00 → Bibliotecas Digitales – VRSV

11:00 a 13:00 → Bibliotecas Digitales – Simulación □omerse□íst

15:00 a 17:00 → Bibliotecas Digitales – *Learningware*

17:00 em adelante → Telemedicina

5. Los días Martes se accederá a las aplicaciones en el siguiente horario:

7:00 a 9:00 → Laboratorios Virtuales – *Learningware*

9:00 a 11:00 → Laboratorios Virtuales – Bibliotecas Digitales

11:00 a 13:00 → Laboratorios Virtuales – VRSV

15:00 a 17:00 → Laboratorios Virtuales – Simulación Distribuida

17:00 en adelante → Telemedicina

6. Los días Miércoles se accederá a las aplicaciones en el siguiente horario:

7:00 a 9:00 → VRSV – Simulación Distribuida

9:00 a 11:00 → VRSV – Laboratorios Virtuales

11:00 a 13:00 → VRSV – *Learningware*

15:00 a 17:00 → VRSV – Bibliotecas Digitales

17:00 en adelante → Telemedicina

7. Los días Jueves se accederá a las aplicaciones en el siguiente horario:

7:00 a 9:00 → Simulación Distribuida – Bibliotecas Digitales

9:00 a 11:00 → Simulación Distribuida – *Learningware*

11:00 a 13:00 → Simulación Distribuida – Laboratorios Virtuales

15:00 a 17:00 → Simulación Distribuida – VRSV

17:00 en adelante → Telemedicina

8. Los días Viernes se accederá a las aplicaciones en el siguiente horario:

7:00 a 9:00 → *Learningware* – VRSV

9:00 a 11:00 → *Learningware* – Simulación Distribuida

11:00 a 13:00 → *Learningware* – Bibliotecas Digitales

15:00 a 17:00 → *Learningware* – Laboratorios Virtuales

17:00 en adelante → Telemedicina

9. Si se requiere utilizar la red avanzada, para actividades que no requieren el uso de las aplicaciones, previa autorización del personal encargado de la administración de la red avanzada, se podrá realizar en el horario de 13:00 a 15:00 de Lunes a Viernes.

10. El uso de la red avanzada será exclusivo para fines educativos y de investigación, así que permanecerá monitorizada de 7:00 a 19:00 por el personal encargado de la administración de la red.

3.4 TOPOLOGÍA FÍSICA DE LA RED

Se recomienda que un miembro tipo de CEDIA posea:

- Una topología física tipo árbol, en la cual se tiene un nodo de enlace troncal desde el cual se ramifican los demás nodos.

Las principales ventajas de la topología en árbol son:

- Es de fácil instalación y mantenimiento.
- Es sencillo conectar nuevos dispositivos.
- No existen elementos centrales de los que dependa toda la red, cuyo fallo dejaría inoperativas todas las estaciones de trabajo.

Para el diseño, se propone que físicamente la red esté constituída de la siguiente manera:

- Se disponga de un enrutador de acceso, el cual, proporciona la conexión a la red externa.
- El enrutador externo está conectado a un *switch*, el cual, es el nodo de enlace troncal de la red.
- Del nodo de enlace troncal se derivan ramificaciones y de éstas pueden desprenderse otras.

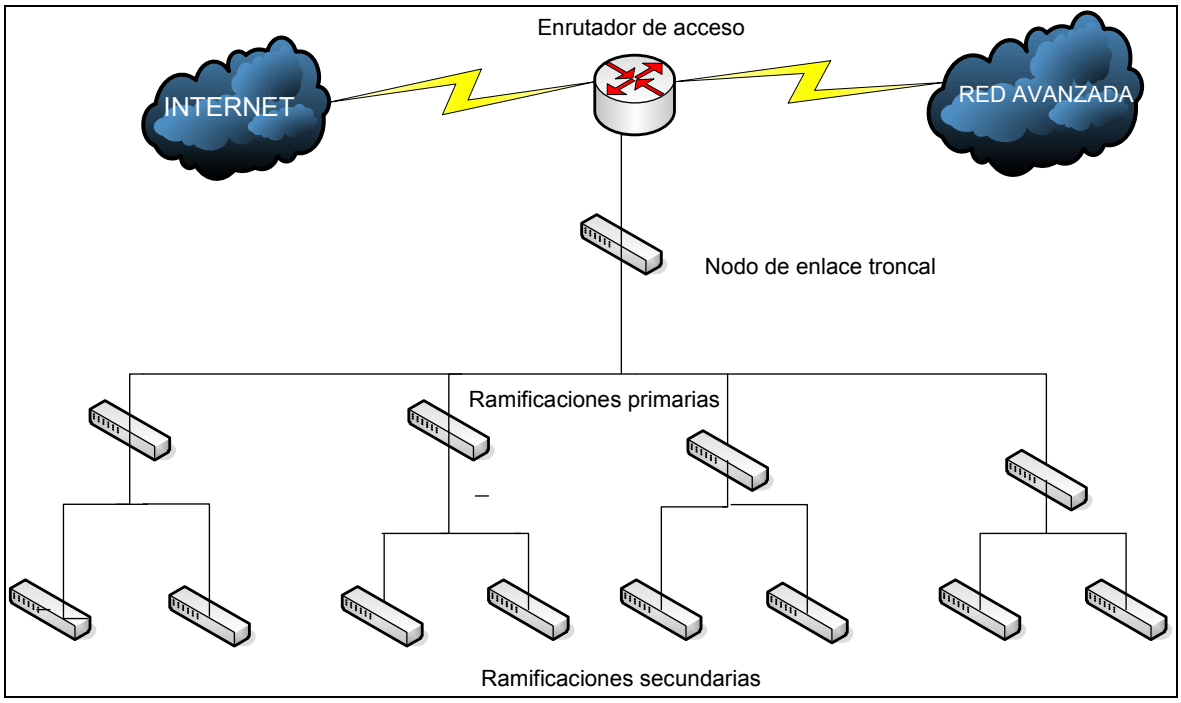


Figura 3.17 Topología física de un miembro tipo de CEDIA

3.5 CARACTERÍSTICAS DE LOS EQUIPOS DE INTERCONEXIÓN DE ACUERDO A LAS NECESIDADES Y LOS ESTÁNDARES A UTILIZARSE

En la actualidad la infraestructura operacional de CEDIA cuenta con una plataforma de red amplia basada en el protocolo Ipv6 el cual trabaja paralelamente con Ipv4. El proveedor de portadora, en este caso Telconet, lo hace posible a través de la configuración de túneles, uno para Ipv6 y otro para *multicast* sobre Ipv4. La infraestructura *multicast* permite establecer una transmisión de videoconferencia de alto desempeño.

La solución a través de túneles provoca *overhead* en el túnel, explicado en términos técnicos generalmente se debe a que el MSS (*Maximun Segment Size*) del túnel GRE (*Generic Routing Encapsulation*) es menor al MTU (*Maximum Transfer Unit*) de los nodos.

El MTU en las redes *Ethernet* es igual a 1500 bytes, el túnel GRE agrega 24 bytes a un paquete, por lo tanto el MSS es igual a:

1500 bytes – 24 bytes = 1476 bytes

Como se puede observar se obtiene un valor de MSS menor al MTU.

Para hacer posible la transmisión es necesario fragmentar los paquetes, lo cual hace que las aplicaciones no trabajen de forma óptima y se degraden las características de desempeño del protocolo IPV6, ya que en el receptor la des-fragmentación no es la adecuada, la solución sería utilizar MPLS (*Multi Protocol Label Switching*), pero, debido a la dependencia del proveedor, este diseño se integrará a la infraestructura existente sin interferir significativamente con los servicios presentes.

Luego del estudio realizado de las aplicaciones de las redes avanzadas, se puede llegar a la conclusión que los equipos de interconexión deben soportar ciertos protocolos y tecnologías para permitir el correcto funcionamiento de las mismas.

Enrutador

El enrutador, al ser el equipo encargado de la interconexión con redes externas, debe soportar principalmente:

- *Dual stack* (protocolos nativos Ipv4 e Ipv6).
- Protocolo de enrutamiento dinámico BGP (*Border Gateway Protocol*).
- Estándar H.323
- Tecnología *Multicast* .

- Protocolo IGMP.
- Protocolo PIM-SM.
- Protocolo MPLS, para garantizar que el equipo pueda ser utilizado el momento en que se lleve a cabo la implementación de este protocolo en la red avanzada ecuatoriana.

Además debe tener las siguientes características en *hardware*:

- Al menos 3 puertos 10 Base-T/100 Base-TX/100 Base-T.
- RAM de al menos 64 MB.
- FLASH de al menos 32 MB.

En el mercado existen muchos productos que cumplen con estas □omerse□ísticas, entre los principales se tiene:

Fabricante	***Productos***
CISCO	Routers, a partir de IOS *(Inter Operating System) Services*
3Com	*Routers* 6000 *family*
Nortel	*Secure router* 4134
Hitache	Familia de *routers* GR2000 *Enhanced version*
Juniper	E-Series *routers*

De las opciones anteriormente mencionadas, el enrutador que se recomienda es de la casa fabricante CISCO, considerando el siguiente criterio:

- La mayoría de miembros de CEDIA, posee actualmente enrutadores CISCO y la experencia con los mismos ha sido satisfactoria.

- Es amplia la disponibilidad en el mercado ecuatoriano de estos equipos, lo que conduce a tener precios competitivos en el mercado.

- Garantía y soporte directos del proveedor.

- Gran cantidad de personal calificado para el manejo de los equipos, debido a las academias instituídas en el país.

El enrutador que actualmente poseen la mayoría de miembros de CEDIA es el CISCO 1811, por lo que, se sugiere la serie 2800 que posee características superiores.

El Cisco 2811 ofrece soporte para las tareas de las redes corporativas que necesitan llevarse a cabo no solo rápidamente sino con un alto nivel de seguridad, permite además mejorar la productividad y disminuir costos a través de la transmisión de señales de voz y video.

Para su uso CISCO recomienda:

Platform	Software Product Description	Image File Name	Part Number	Recommended Flash (in Megabytes)	Recommended DRAM (in Megabytes)
Cisco 2811	ADVANCED IP SERVICES	c2811-advipservicesk9-mz	S280AISK9-12308T	64	256

Figura 3.18 CISCO 2811[39]

Entre las características más destacadas de este enrutador se tiene:

- Memoria RAM: 256 MB (instalados) / 768 MB (máx.)
- Memoria Flash: 64 MB (instalados) / 256 MB (máx.)
- Tecnología de red: Ethernet, Fast Ethernet, Gigabit Ethernet
- Red / Protocolo de transporte: IPSec
- Protocolo de gestión remota: SNMP 3
- Indicadores de estado: Actividad de enlace, alimentación
- Cumplimiento de los estándares DES, 3DES, AES 128, AES 192 y AES 256.
- Protección *firewall*, cifrado del *hardware*, asistencia técnica VPN, filtrado de URL

El IOS que posee el perfil requerido para un miembro tipo de CEDIA es el Cisco IOS XR *Software Release* 3.3, se puede destacar de sus características:

1. *Multiprotocol* BGP (MP-BGP)
2. H.323 con NAPT (*Network Address Port Translator*)
3. *Multicast* IPv4 e IPv6
4. MPLS VPNs , lo cual permite poseer una plataforma con servicios IP de alto desarrollo, intranets, voz, multimedia y *network commerce*, ofrece

además privacidad, seguridad, escalabilidad, fácil integración con otras intranets.

El soporte MPLS es importante, ya que, es necesario proyectarse al futuro, puesto que el pertenecer a una red avanzada compromete a ir de la mano con el avance tecnológico.

Según el Coordinador de Grupos de Tecnología de CLARA el Ing. Ivan Morales, en las reuniones técnicas se ha resaltado el hecho de que muchas redes avanzadas latinoamericanas, tienen problemas de disponibilidad de equipos de enrutamiento.

La red avanzada ecuatoriana no es la excepción en esta problemática, por lo que se mencionará otra opción de equipo de enrutamiento basada en ***Open Source*** a través de programas de enrutamiento que ofrecen funcionalidades similares a las de un enrutador en *hardware.*

En la Red Avanzada Guatemalteca de Investigación y Educación (RAGIE) se optó por usar *software* de código abierto para el enrutamiento, obteniendo muy buenos resultados.

Entre el principal *software* a nuestra disposición tenemos:

- Vyatta.
- Xorp (*eXtensible Open Router Platform*).
- Quagga.

La primera opción es un CD tipo *appliance* de ruteo que posee un costo según la versión a utilizarse, las dos siguientes son *software* de ruteo que se pueden instalar sobre Linux o FreeBSD.

Quagga es un *software* de ruteo con licenciamiento GPL (*General Public License*) que puede ser instalado sobre Linux o *FreeBSD*, provee de enrutamiento basado en TCP/IP, soporta los protocolos:

- RIP (versión 1, versión 2, versión ng)
- OSPF (versión 2, versión 3)
- BGP (-4, -4+)
- *Special* BGP (*Route Reflector y Route Server*)

Soporta también protocolos de ruteo IPv6 y administración via SNMP, provee de alta calidad y una interfaz de usuario para cada protocolo de enrutamiento.

A pesar de ser muy buenas las opciones anteriormente mencionadas, éstas no soportan la tecnología *Multicast* en la actualidad, por lo que se recomienda el uso de XORP.

XORP es una plataforma de enrutamiento de código abierto, da soporte a protocolos enrutados IPv4 e IPv6, integra además soporte a *multicast*. Posee licenciamiento BSD.

Está disponible a descargarse como un Live CD ó Código Abierto.

Live CD es una imagen del disco que se encuentra disponible en http://www.xorp.org/releases/1.4/LiveCD.iso.gz , pesa alrededor de 109 MB, y provee la facilidad de no tener que compilar nada, ni formatear el disco duro o la computadora a diferencia del código abierto.

Si se desea instalar XORP a través del código, se puede escoger la versión que se adapte a los requerimientos, en la dirección electrónica:

http://www.xorp.org/downloads.htm

Entre los requisitos de usuario se tiene:

- 1.4 GB libres en disco duro.
- El código puede ser compilado sobre Linux 2.4.x, Linux 2.6.x, DragonFlyBSD, FreeBSD, NetBSD, OpenBSD, MacOS X y Windows Server 2003.
- De preferencia se recomienda el sistema operativo FreeBSD 4.x, ya que sobre éste fue desarrollado XORP.

Con XORP se pueden configurar rutas estáticas o protocolos de enrutamiento tales como: RIP (*Routing Information Protocol*), OSPF (*Open Shortest Path First*), BGP (*Border Gateway Protocol*).

Para el soporte *multicast* deberá ser configurado el MFEA (*Multicast Forwarding Engine Abstraction*).

Se tiene además soporte para los protocolos utilizados para *multicast*: IGMP (*Internet Group Management Protocol*) utilizado en *multicast* sobre IPv4, MLD (*Multicast Listener Discovery*) para *multicast* sobre IPv6 y PIM-SM (*Protocol Independent Multicast - Sparse Mode*).

Para el soporte del protocolo H.323 en cualquier sistema GNU/Linux, el procedimiento a realizarse es instalar OpenH323, que igualmente es *software* de libre distribución, más información la podemos encontrar en:

http://www.openh323.org/

Se recomienda instalar primeramente la librería **pwlib-1.10.10** y luego **openh323_v1_18_0**, que son las versiones estables y no dan problemas en la compilación.

- Para la configuración del software: **./configure**
- Para la compilación: **./make**
- Para la instalación: **./make install**

Los requisitos para su uso son el poseer una computadora dedicada únicamente a la función de enrutamiento con las siguientes características mínimas:

- Procesador Pentium IV de 1.8 GHz.
- Memoria RAM de 512 MB.
- 20 GB de espacio libre en disco duro.
- 2 tarjetas de red (1 para la red CEDIA y otra para la red interna).

En cuanto al *software* a utilizarse en las máquinas de los usuarios, actualmente la mayoría ya tiene soporte a IPv6, así se tiene:

Fabricante	Sistema Operativo
Macintosh	Mac OS X 10.2 Jaguar
Unix	AIX 4.3
	Tru64 UNIX 4.0D (de Compaq)
	Tru64 UNIX 5.1 (de Compaq)
	FreeBSD 4.0
	Linux kernel 2.0 o recientes
	NetBSD 1.5
	OpenBSD 2.7 o recientes
	Solaris 8
	HP-UX 11i Ipv6 (de Hewlett Packard)
Microsoft	Windows 2000
	Windows XP
	Windows Vista

Tabla 3.6 Soporte IPv6

Para aprovechar los recursos existentes en la conformación de una nueva red local que accederá a la red avanzada, se recomienda la configuración de redes locales virtuales o VLANs, de esta manera los equipos pertenecientes a las redes IPv4 e IPv6 se pueden encontrar en distintos sectores y se conectarán al mismo medio físico, en este caso al mismo *switch*.

Se mostrará un ejemplo en las figuras 3.19 y 3.20:

Switch

El *switch* a utilizarse deberá ser administrable, para la configuración de las VLANs.

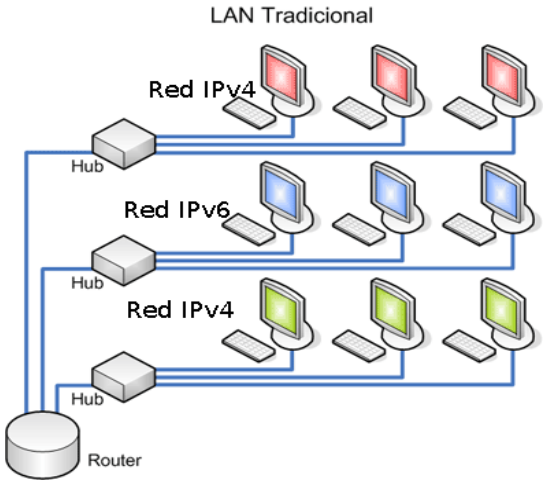


Figura 3.19 LAN tradicional [40]

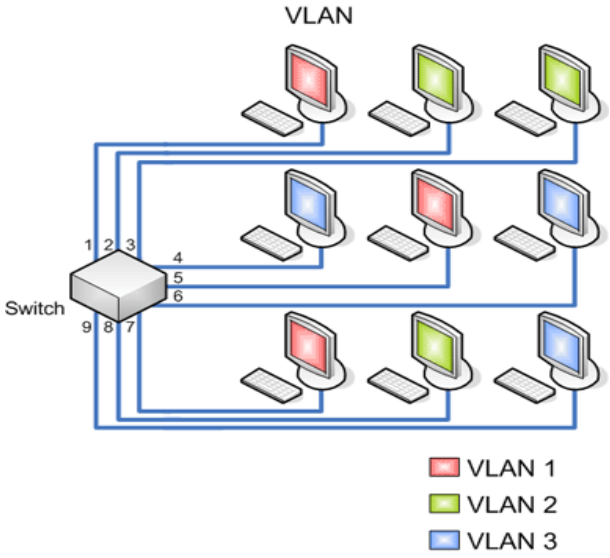


Figura 3.20 VLANs [40]

Entre las principales características que deberá poseer el *switch* se tienen:

- 48 puertos 10/100 BASE-T.
- Al menos un puerto 1000 BASE-T.

En el mercado se tienen muchos productos que cumplen con estas caracterísitcas, entre los principales se tiene:

Fabricante	***Productos***
CISCO	Catalyst 2950T
3Com	SS4 5500
DLINK	DES-3052

Se sugiere la utilización del *switch* marca Cisco debido a que se desea mantener la compatibilidad entre equipos de *networking*. Esto hace que la convergencia de la red sea más rápida y el trabajo de la misma sea óptimo.

Figura 3.21 Switch CISCO Catalyst 2950T-48 [41]

3.6 CABLEADO ESTRUCTURADO

El sistema de cableado estructurado de la LAN de un miembro tipo de la red CEDIA deberá consistir en una infraestructura flexible que pueda aceptar y soportar sistemas de datos y de voz múltiples.

Se recomienda como mínimo la utilización del cable UTP categoría 5e, el cual permite transmitir datos a velocidades alrededor de 1000 Mbps.

3.6.1 NORMAS

Debido a que el diseño va orientado a un miembro tipo, del cual no se tienen características de sus instalaciones, no se puede diseñar el sistema de cableado

estructurado, ya que éste depende exclusivamente de la infraestructura física del miembro. Por lo tanto, se sugiere que se cumplan las principales normas existentes para el cableado.

El cumplimiento de las normas permitirá eliminar la necesidad de seguir las reglas de un proveedor en particular, qué tipos de cable, conectores, distancias, o topologías utilizar.

El cableado estructurado es instalado una sola vez, permitiendo su adaptación a nuevas tecnologías en el futuro.

El cableado estructurado está compuesto por los siguintes subsistemas:

1. **Instalación de entrada, o acometida**

   Punto donde la instalación exterior y dispositivos asociados entran al edificio, puede estar utilizado por otras redes públicas, redes privadas del cliente, o ambas, aquí se encuentran ubicados además los dispositivos de protección para sobrecargas de voltaje.

2. **Sala de máquinas o equipos**

   Es un espacio centralizado para el equipo de telecomunicaciones.

3. **Cableado Vertical**

   Proporciona interconexión entre los gabinetes de telecomunicaciones.

4. **Gabinete de telecomunicaciones**

   Es donde terminan los conectores compatibles de los cables de distribución horizontal.

5. **El cableado horizontal**

   Medio físico usado para conectar cada toma o salida a un gabinete. Se pueden usar varios tipos de cable.

6. **El área de trabajo**

   Unión de la toma o salida al equipo o estación de trabajo del usuario.

La norma ANSI/TIA/EIA-569-A especifica los criterios técnicos para la instalación de los subsistemas de cableado estructurado.

ANSI/EIA/TIA-569-A

"Norma de construcción comercial para vías y espacios de telecomunicaciones".

La cual da un criterio para ubicaciones, áreas, y vías a través de las cuales se instalan los equipos y medios de telecomunicaciones.

Otras normas principales para la implementación de un sistema de cableado estructurado son:

ANSI/TIA/EIA-568-B

"Norma para construcción comercial de cableado de telecomunicaciones".

Mediante esta norma se tendrán los criterios técnicos y de rendimiento para la instalación de componentes y configuraciones de sistemas.

ANSI/TIA/EIA-606-A

"Norma de administración para la infraestructura de telecomunicaciones en edificios comerciales".

Proporciona normas para la codificación de colores, etiquetado, y documentación de un sistema de cableado instalado, esto facilitará la localización de fallas.

ANSI/TIA/EIA-607-A

"Requisitos de aterrizado y protección para telecomunicaciones en edificios comerciales".

Permite tener una conexión a tierra confiable, para todos los equipos.

3.7 *SOFTWARE* A UTILIZARSE

3.7.1 BIBLIOTECAS DIGITALES

***Software* necesario:**

Para acceder a las bibliotecas digitales se requiere únicamente de un navegador ya sea:

- Internet *Explorer* versión 4.0 o superior
- *Netscape Communicator* también en versión 4.0,
- *Mozzila Firefox*, entre otros.

Para poder visualizar los archivos que se encuentren en formato pdf se requiere:

- Adobe Acrobat Reader versión 3.0 o superior.

En caso de que la biblioteca utilizase otro formato para el almacenamiento digital del texto, el usuario deberá descargar el *software* pertinente para poder disponer de la información.

En el caso de los *talking books*, se requiere de un reproductor de audio y video, que decodifique el formato mp3, con el que están codificados los libros.

- *Windows Media Player*
- *Winnamp*
- *Power* DVD
- *Quick Time*

Para el audio y video el usuario deberá utilizar de igual manera cualquier programa mencionado anteriormente.

3.7.2 TELE-INMERSIÓN [8]

A pesar de que la tele-inmersión es una aplicación que no puede ser implementada en la red avanzada ecuatoriana en la actualidad, debido a las limitaciones del enlace, se mencionarán los requisitos necesarios en *software* con el fin, de que sirva de guía para el futuro.

El *software* deberán incluir características generales como:

- Un sistema 3D en tiempo real para capturar de forma dinámica objetos reales.
- Capturador de escenas estáticas.

- Un sistema que permita crear en forma automática una imagen de acuerdo a un modelo tridimensional.
- Manipulación y modelado de objetos virtuales.
- Una arquitectura que permita la interacción y colaboración multi-persona, entre otras características.

Emisión

Sistema de modelado 3D

Software que manipula las imágenes capturadas, para analizarlas entre si, combinarlas con mapas de profundidad y corregir errores, consiguiendo de esta manera imágenes estereoscópicas en 3D.

Algoritmos de compresión

Reducen el tamaño en *bytes* de las imágenes previa a la transmisión

Recepción

Algoritmos de descomprensión y renderizado[7]

Descomprimen la información y reconstruyen las imágenes.

[7] Renderizado: La palabra *renderización* proviene del inglés *render*, y no existe un verbo con el mismo significado en español, por lo que es frecuente usar las expresiones *renderizar* o *renderear*. En el proceso de renderización, la computadora "interpreta" la escena en tres dimensiones y la plasma en una imagen bidimensional.

3.7.3 LABORATORIOS VIRTUALES

En el acceso a un laboratorio virtual se requiere de un navegador ya sea:

- Internet *Explorer* versión 4.0 o superior
- *Netscape Communicator* también en versión 4.0,
- *Mozzila Firefox*, entre otros.

Una vez que se ha accedido al laboratorio virtual se pueden enviar datos, simular imágenes en 2D, consultar resultados, entre otras actividades, mediante el mismo navegador.

En el caso que se desee reproducir un video pre-grabado de alguna sesión o pruebas realizadas, se puede utilizar cualquier reproductor de video, siempre y cuando soporten el formato del video. Entre los más comunes se tiene:

- Windows Media Player
- DivX Placer
- WinDVD
- Winamp
- Real Player, entre otros

3.7.4 TELEMEDICINA

El uso de la telemedicina, como se mencionó anteriormente, requiere de la transmisión de texto, imágenes de alta calidad, acceso a bases de datos y establecimientos de videoconferencias.

En la transmisión de datos, por lo general, se accede via *web* a servidores FTP a través de los cuales se puede enviar o recibir archivos, de igual manera en el acceso a bases de datos, se posee una interfaz *web* de la base de datos y a través de ésta se ingresa y se obtiene información, por lo tanto, para este tipo de actividades se requerirá de un navegador, entre los principales se mencionarán:

- Internet *Explorer* versión 4.0 o superior
- *Netscape Communicator* también en versión 4.0,
- *Mozzila Firefox*, entre otros.

Para el establecimiento de una videoconferencia se requiere de un cliente para videoconferencias H323:

- *Polycom ViewStation,*
- *Polycom ViaVideo*,
- *Microsoft NetMeeting,*
- CUseeMe,

Existen en la actualidad clientes H.323 de código abierto, así se tiene:

- OhPhone , un cliente H.323 en modo texto.
- Open Phone, un cliente H.323 de interfaz gráfica (Disponible actualmente para Windows).

3.7.5 VRSV

Se requiere del cliente de videoconferencia para el establecimiento de la misma:

- *Polycom ViewStation,*
- *Polycom ViaVideo*,
- *Microsoft NetMeeting,*
- CUseeMe,
- OhPhone,
- Open Phone, entre otros.

En el caso de que se acceda al Chat de las VRSVs se utilizará principalmente:

- Skype

3.7.6 *LEARNINGWARE* O *SOFTWARE* DE APRENDIZAJE

Software para el cliente *web*:

- Intenet *Explorer* versión 5.5 o superior.
- *Netscape* 6.0 o superior.
- *Mozzila Firefox*, entre otros.

En el caso que se desee reproducir audio, se puede utilizar cualquier reproductor de audio, siempre y cuando soporten el formato del archivo. Entre los más comúnes se tiene:

- Windows Media Player
- Winamp
- Music Match Jukebox,

- Amarok,
- Real Player, entre otros.

- **Procesador de Palabras**:

Un procesador de palabras es necesario para todo estudiante.

Los estudiantes que estudian en línea deben estar preparados para guardar archivos como texto o documentos, saber utilizar la función de *“copy”* y *“paste”* de esta manera se podrá incluir el trabajo en los mensajes de *e-mail*.

Se debe también conocer los procedimientos de adjuntar trabajos realizados en el procesador de palabras a un *e-mail*.

- **Programa específico de algún curso**

Otros programas como parte de los requisitos del curso. La mayoría de éstos son completamente gratis.

Los programas más utilizados por los sistemas de enseñanza son:

- *Acrobat Reader.*
- *Real One Player.*
- *Quicktime.*
- *Shockwave and Flash*

3.7.7 SIMULACIÓN DISTRIBUIDA

Esta aplicación requiere de *software* especializado en un campo del conocimiento, existen en el mercado un sin número de sistemas computacionales que pueden ser de código abierto o propietario. Entre los principales se puede mencionar:

- Globus Toolkit, producto de Globus Alliance, el cual permite compartir recursos computacionales relacionados a las ciencias exactas,

- Cluster Express, producto de Grid, permite monitorear, administrar y acceder remotamente a un *cluster*,

- BOINC, producto de Climate Prediction, que permite predecir el clima,

- Entre otros.

3.8 PRESUPUESTO

A continuación se detallará el costo de implementación de los equipos necesarios para además de permitir el acceso a la red avanzada CEDIA, dar soporte a todas las aplicaciones y protocolos que no son posibles de utilizar a través del Internet comercial.

Cabe recalcar que se realizará el análisis de los elementos necesarios únicamente para la instalación de los equipos que permitirán el acceso a la red avanzada, esto debido a que cada miembro posee su red interna ya instalada y el presupuesto lo ajustarán de acuerdo a sus necesidades.

3.8.1 USO DE ROUTER CISCO

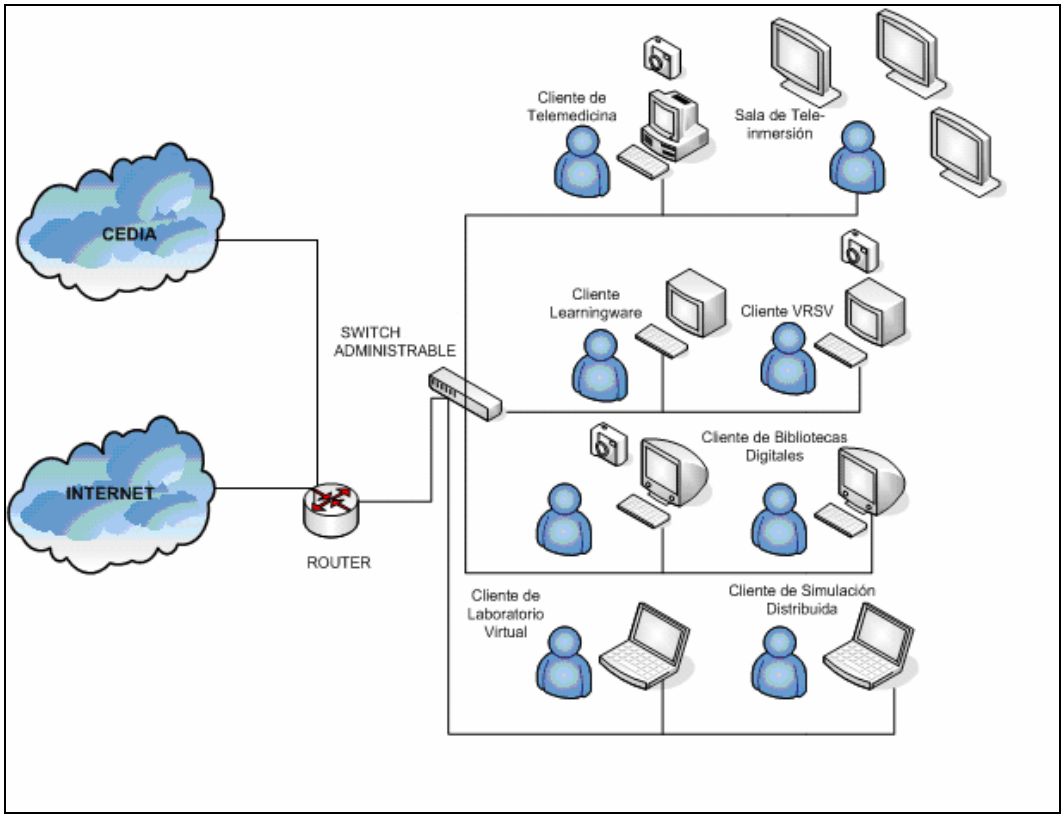


Figura 3.22 Infraestructura de Red

Elemento	Cantidad	Valor total
Enrutador CISCO 2811	1	$2400
Software Cisco IOS ADVANCED IP SERVICES	1	$1904
Recursos Humanos	1	$1000
Switch CISCO Catalyst 2950T	1	$1484
Imprevistos		$100
TOTAL		$6888

Tabla 3.7 Presupuesto con la compra de un router CISCO

Todos los valores incluyen impuestos.

No se ha tomado en cuenta el costo de la configuración del equipo ya que este valor va incluido en el asignado a los recursos humanos.

Se ha considerado el presupuesto que deberá asignar un miembro tipo de CEDIA para la instalación del equipamiento de interconexión, asumiendo que el mantenimiento de los mismos se realizará por parte del personal técnico o del área de ingeniería perteneciente a la institución miembro.

3.8.2 USO DE SOFTWARE DE RUTEO XORP

Se considera necesario mencionar un presupuesto, en el caso de que el miembro tipo de CEDIA se incline por el uso de *Open* Source.

Elemento	Cantidad	Valor total
Software Xorp	1	$0.00
Software Open H323	1	$0.00
Servidor (Procesador Pentium IV de 1.8 GHz, Memoria RAM de 512 MB, 40 GB de Disco Duro, 3 Tarjetas de Red)	1	$1000
Recursos Humanos	1	$1000
Switch CISCO Catalyst 2950T	1	$1484
Imprevistos		$100
TOTAL		$3584

Tabla 3.8 Presupuesto con Open Source

El presupuesto presentado se enfoca a la parte de acceso a la red, ya que para los usuarios es necesaria una inversión adicional. Para la mayoría de aplicaciones el usuario requiere de un computador que debe tener como mínimo los siguientes elementos y caracterísitcas:

- Procesador Pentium IV,
- 1.8 GHz de procesamiento,
- 256 MB RAM,
- 40GB en disco duro,
- licenciamiento Windows XP,
- teclado,
- *mouse*,
- monitor,
- microfono,
- webcam,
- parlantes.

El costo aproximado de un computador de estas características está alrededor entre los 600 dólares.

En el caso de que se requiera licenciamiento de *software* adicional, el costo dependerá del producto que se desee adquirir.

Adicionalmente para el caso de la Tele-inmersión se requiere un sistema completo y complejo para el cliente, el mismo que tiene un costo que va desde los 30000 dólares en adelante, dependiendo de las características del sistema.

No se lo ha incluido en el presupuesto general debido a que esta aplicación en la actualidad no puede ser implementada debido a la falta de recursos de red.

4 PLANTEAMIENTO DE UNA ALTERNATIVA DE CONECTIVIDAD

4.1 PLANTEAMIENTO DE LA ALTERNATIVA DE CONECTIVIDAD

Se tienen estadísticas del porcentaje de pérdida de conexión con la red avanzada de cada uno de los miembros. Como se puede observar en la figura 4.1 existen casos críticos como el Instituto Nacional de Pesca, ante esta situación surge la necesidad de plantear una alternativa de conexión que permita a los miembros seguir comunicados con CEDIA.

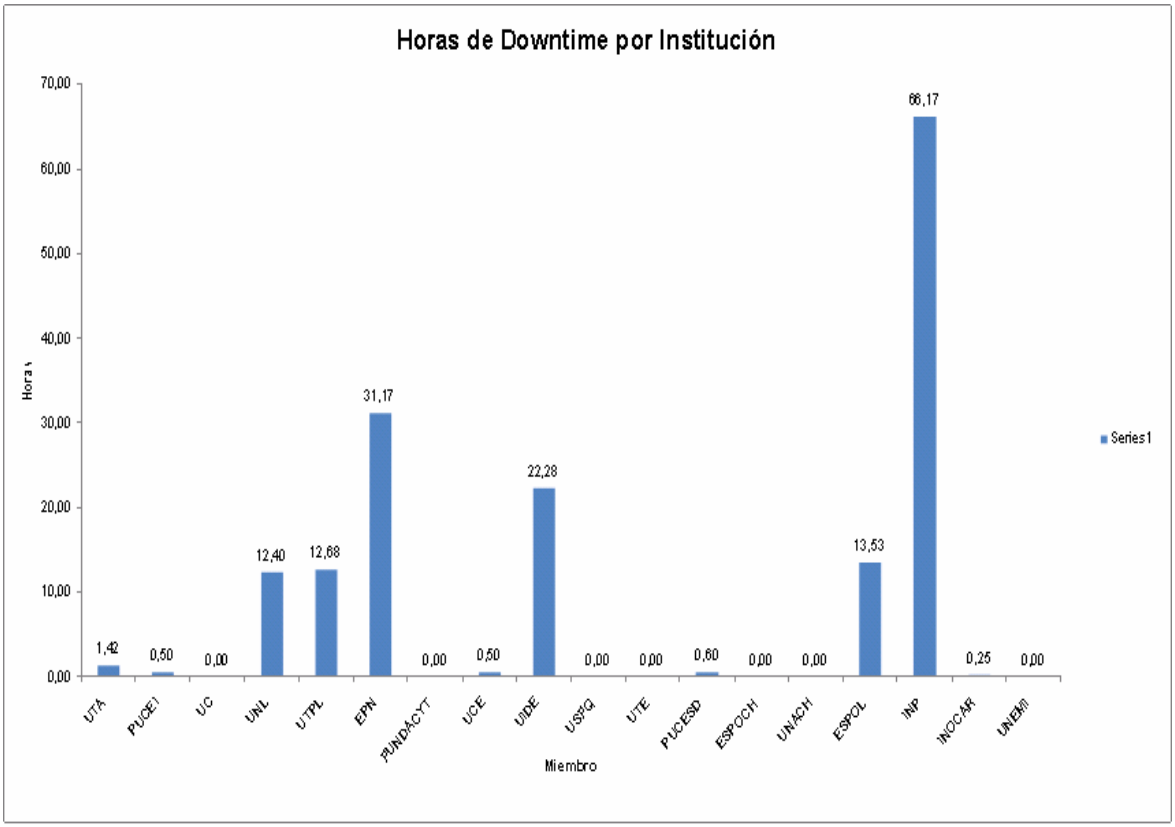


Figura 4.1 Estadísticas de caidas del Servicio en el 2007

La estructura actual de la red CEDIA está conformada de manera que la conexión al Internet comercial y a la red avanzada son contratadas por separado, en el capítulo 1 sección 1.3 se menciona las capacidades contratadas por cada miembro.

Debido a que no existe un enlace redundante para el acceso a la red avanzada, ya que esto significaría un aporte adicional por parte de todos quienes conforman CEDIA, se sugiere la posibilidad de establecer conexión entre los miembros con similares características a través del Internet comercial, lo que luego de su implementación se consideraría no solo una alternativa para quienes pierdan conectividad, sino también una solución para aquellos que no puedan acceder mediante un enlace dedicado.

Una solución similar tiene implementada la red CUDI (Corporación Universitaria para el Desarrollo de Internet) de México, la cual ha dado buenos resultados en sus operaciones.

Se debe tomar muy en cuenta que el acceso a través de una red pública debe garantizar:

- Seguridad
- Confiabilidad
- Confidencialidad
- Integridad

Para lograr estos objetivos, el sistema a utilizarse deberá proveer de:

- Autorización
- Autenticación

- Registro

Estas características las provee la tecnología VPN (*Virtual Private Network*) a través de un esquema basado en la encriptación haciendo uso de algoritmos de cifrado como *Data Encryption Standard* (DES), *Triple DES* (3DES) y *Advanced Encryption Standard* (AES) para garantizar la confidencialidad, algoritmos *Message Digest* (MD2 y MD5), *Secure Hash Algorithm* (SHA) que permiten garantizar la integridad de los datos y la autenticación para permitir el acceso asegurando que nunca se restrinja para usuarios autorizados.

Otro de los principales motivos por el que se eligió el uso de esta tecnología es la reducción de costos comparado con la contratación de un enlace dedicado redundante.

Tenemos 3 arquitecturas de conexión VPN a nuestra disposición:

- VPN de acceso remoto:

Consiste en la conexión de los usuarios desde un sitio remoto a un servidor VPN.

- VPN punto a punto:

Consiste en la conexión entre servidores VPN.

- VPN interna WLAN:

Consiste en aislar zonas y servicios usando la misma red interna.

Se puede concluir que la opción que más se adapta a la realidad de la red avanzada ecuatoriana, es el establecimiento de una VPN punto a punto, debido a que la conexión va a ser establecida entre dos miembros y además debe ser trasparente para el usuario.

Con respecto a la implementación de la red privada virtual, se tiene en la actualidad 3 opciones:

- Soluciones basadas en *hardware*
- Soluciones basadas en *firewall*
- Soluciones basadas en *software*

Soluciones basadas en *hardware*

Debido a que su diseño es específico para las funciones a realizarse, las soluciones basadas en *hardware* ofrecen mayor rendimiento y facilidad de configuración.

Entre las marcas más conocidas se tiene:

Nortel, Cisco, Linksys, Netscreen, Symantec, Nokia, US Robotics, D-link

Soluciones basadas en *firewall*

Su ventaja es la seguridad que brinda el *firewall*, pero se obtiene un menor rendimiento debido a la carga en procesamiento. Generalmente se usa *hardware* adicional para liberar consumo en procesamiento, por ejemplo: *Cisco Pix, Checkpoint NG.*

Soluciones basadas en *software*

Ofrecen mayor flexibilidad ya que son re-configurables y se pueden adaptar a nuevos modelos de interoperatividad.

Para los sistemas operativos más conocidos como son: *Windows, GNU/Linux y Unix* se tiene el siguiente *software* de código abierto:

- *OpenSSH (Open Secure Shell)*
- *OpenVPN*
- *FreeS/Wan*

La solución que se recomienda es la basada en *software open source*, ya que ofrece similar funcionalidad de las anteriores, pero con la diferencia de que el costo adicional por implementación es menor.

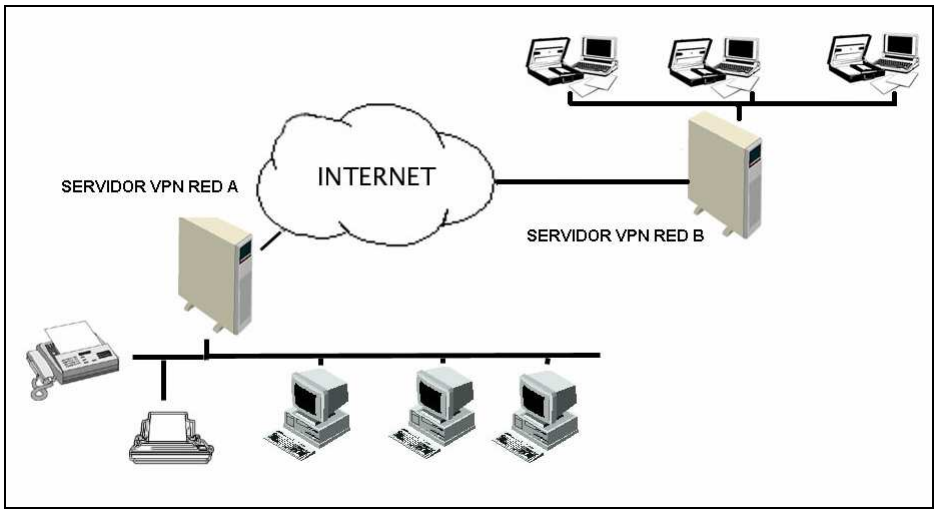


Figura 4.2 Esquema de VPN punto a punto

Se poseen varias opciones en cuanto al protocolo a utilizarse para el establecimiento de la red privada virtual, entre los cuales se mencionan:

- PPTP (*Point to Point Tunneling Protocol*)
- L2F (*Layer 2 Forwarding*)
- L2TP (*Layer 2 Tunneling Protocol*)
- IPSec (*Internet Protocol Security*)

Se ha escogido el protocolo IPSec debido a sus ventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados.

4.1.1 IPSEC (*INTERNET PROTOCOL SECURITY*) [43]

Es un estándar que proporciona servicios de seguridad a la capa IP y a todos los protocolos supriores (TCP y UDP, entre otros). Entre las ventajas de IPSec se destaca que proporciona un nivel de seguridad común y homogénea para todas las aplicaciones, además de ser independiente de la tecnología física empleada.

Está basado en un modelo de seguridad extremo a extremo, lo que significa que los únicos *host*s o enrutadores que tienen que conocer la protección de IPSec son el que envía y el que recibe. Cada equipo controla la seguridad por sí mismo en su extremo, bajo la hipótesis de que el medio por el que se establece la comunicación no es seguro.

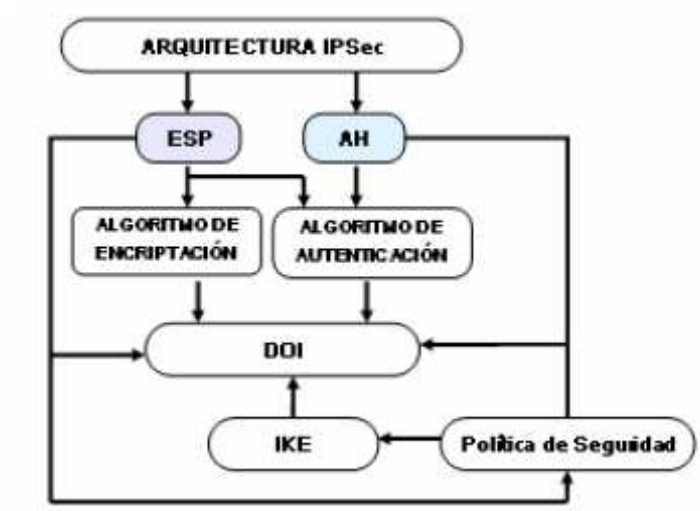


Figura 4.3 Arquitectura IPSec [43]

Al utilizar el protocolo AH (*Authentication Header*) se aplican algoritmos de autenticación de los datos (la información enviada es realmente de quien dice ser) y al emplear el protocolo ESP (*Encapsulating Security Payload*) se aplican algoritmos de encriptación con flexibilidad para soportar combinaciones de autenticación, integridad de datos (seguridad de que cualquier alteración de la información será detectada), control de acceso (se establecen políticas de establecimiento de conexiones IPSec) y confidencialidad de datos (la información enviada no será vista por otras personas).

AH (Solo autenticación):

1. Detecta los cambios de contenido.
2. Los destinatarios pueden autenticar el origen.
3. Previene los ataques de *IP-Spoofing*.
4. Protege el ataque de retransmisión.

ESP (Cifrado y si se quiere autenticación):

1. Confidencialidad de contenido.
2. Confidencialidad limitada de flujo de tráfico.
3. Opcionalmente, servicio de autenticación como AH.

DOI (*Domain of Interpretation*) define todos los parámetros que se negocian para establecer canales seguros, incluyendo identificadores únicos para algoritmos de autentificación y de encriptamiento durante el proceso de comunicación.

Además de las medidas necesarias para establecer una conexión AH o ESP, también especifica parámetros operacionales para el protocolo IKE (*Internet Key Exchange*) tales como, tiempo de vigencia de las claves (*key Exchange*) y ubicación de las claves criptográficas.

La Política de Seguridad (*Security Policy*) almacena información adicional para definir qué tráfico proteger y cuándo hacerlo. IPsec funciona a partir de dos políticas de seguridad:

- Base de datos de políticas de seguridad SPD (*Security Policy Database*), estas políticas le dicen a IPSec cuando debe o no actuar sobre un paquete IPv6.

- Base de datos de asociaciones de seguridad SAD (*Security Association Database*), estas asociaciones le dicen a IPSec cómo debe crear el canal entre las dos máquinas.

PROTOCOLO IKE

Es un protocolo de control que se encarga de poner en contacto y negociar los algoritmos, claves y demás elementos para la comunicación segura con IPSec entre dos computadores.

Entre las características más importantes de IPSec se puede destacar:

- IPSec opera en la capa 3 del modelo OSI (*Open System Interconnection*), lo que le permite proteger a los protocolos de las capas superiores, incluyendo TCP (*Transmission Control Protocol*) y UDP (*User Datagram Protocol*), que son los más utilizados.

- Para utilizar IPSec las aplicaciones no tienen que hacer ninguna modificación en su código.

- Para el uso de *Multicast* IPSec proporciona una asociación de seguridad que consiste en un índice de parámetro de seguridad (SPI) y la dirección de destino de la cabecera del paquete, ésta es duplicada a todos los receptores quienes conforman el grupo.

- El uso de IPSec es obligatorio en IPv6.

- Cifra el tráfico transportado.

- Valida la integridad de los datos transmitidos.

- Autentica los extremos que quieren establecer conexión.

- No permite la duplicación de sesiones seguras.

El modo de operación a utilizarse es IPSec modo túnel, ya que éste nos permite obtener una comunicación segura entre enrutadores, en este caso, para la VPN que se ha de establecer.

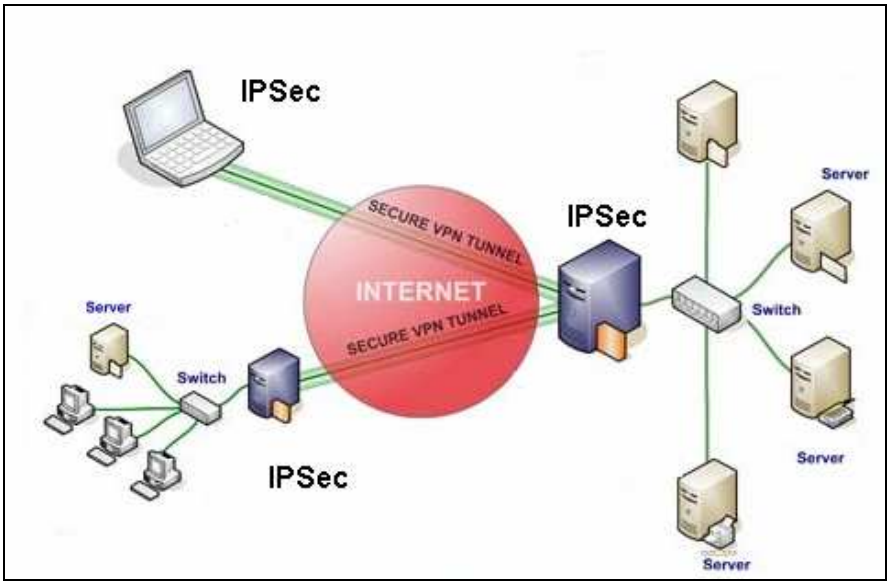


Figura 4.4 Túnel con IPSec

Luego de tener claro como se deben comunicar los nodos a través del Internet comercial, es necesario establecer los porcentajes de utilización de capacidades, se recomienda usar el 50% para el Internet y el 50% restante para la red avanzada, estos valores variarán de acuerdo al criterio y a las necesidades de cada institución.

Para poder obtener niveles de rendimiento aceptables en la conexión alterna, como requisito fundamental se tiene, el tener contratados por lo menos 2048

kbps, con esto garantizamos que si únicamente utilizamos el 50% de la capacidad tendremos 1M para un soporte óptimo de las aplicaciones.

A continuación se detalla nuestro planteamiento, destacando como primer punto la utilización del sistema operativo GNU/Linux sobre el cual se instalarán todos los paquetes de código abierto necesarios que permitan establecer la red privada virtual a través del Internet comercial con todos los parámetros necesarios para transportar tráfico de una red avanzada.

4.1.2 IPV6/IPV4 [44]

El protocolo de red del Internet Comercial es IPv4, por este motivo se necesita un mecanismo que nos permita la utilización de IPv6 sobre la red comercial, aunque los nodos finales, en este caso, los computadores de los miembros de CEDIA soportan IPv6, los enrutadores actuales de Internet descartan los paquetes IPv6.

Para esto existen algunos mecanismos ya implementadas en la actualidad.

A continuación se realizará un breve estudio mecanismos para la interacción de sistemas IPv4 e IPv6 y se elegirá el que mejor se adapte a la situación actual.

Existen dos mecanismos:

- Tipo Túnel
- Tipo Traducción

Tipo Túnel

Se basan en encapsular. Están enfocados en unir dos islas IPv6 a través de un océano IPv4.

Así se tiene:

- Túneles manuales
- Túneles automáticos
- Túneles 6to4
- 6over4

Figura 4.5 Mecanismo de túnel IPv6/IPv4 [44]

Mecanismos de traducción

Se basan en traducir, en un elemento de red, los paquetes de un formato a otro

Así se tiene:

- NAT-PT
- *SOCKSv5*

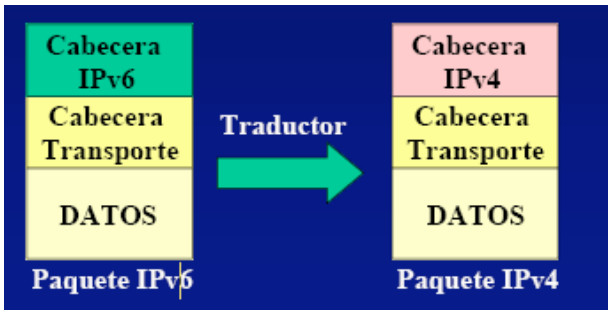


Figura 4.6 Mecanismo de Traducción [44]

4.1.2.1 Túneles Manuales

Características Principales

- Funcionalidad: interconectar islas IPv6 a través de un océano IPv4.
- Cada extremo es un nodo dual y en ellos se configura las direcciones IPv4 e IPv6 tanto local como remotas.

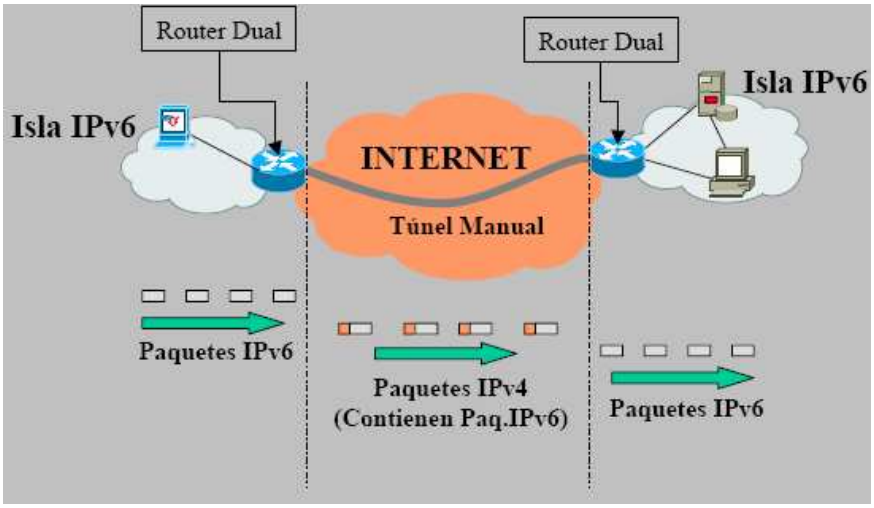


Figura 4.7 Túneles Manuales [44]

Ventajas

- Disponible en multitud de plataformas (Cisco, GNU/Linux, Solaris).
- Método totalmente transparente respecto al nivel IPv6 y superiores con lo cual no afecta a las aplicaciones.
- No consume excesivos recursos, la MTU (*Maximum Transmission Unit*) se reduce en 20 bytes (cabecera IPv4 típica).

Desventajas

- No son dinámicos, se establecen manualmente o de forma semiautomática.

- Si se unen N islas sin considerar un nodo central o intercambiador, el número de túneles en cada sitio sería N-1, es decir si el número de islas es muy grande este método carecería de sentido.

4.1.2.2 Túneles Automáticos

Características principales:

- Permite a nodos duales comunicarse a través de una infraestructura IPv4.
- Direcciones IPv6 “IPv4-Compatible”: Prefijo 0::/96 + dirección IPv4.
- Se define una interfaz virtual para la dirección “IPv4 compatible”.
- Los paquetes destinados a las direcciones “IPv4 Compatible” se envían por el túnel automático.
- Reglas:
    - Dirección origen IPv6: Dirección “IPv4 Compatible” local.
    - Dirección destino IPv4: Extraída de la dirección IPv4 Compatible remota.
- Uso de túneles automáticos y túneles manuales: *Hosts* IPv6 aislados (sin enrutadores IPv6).

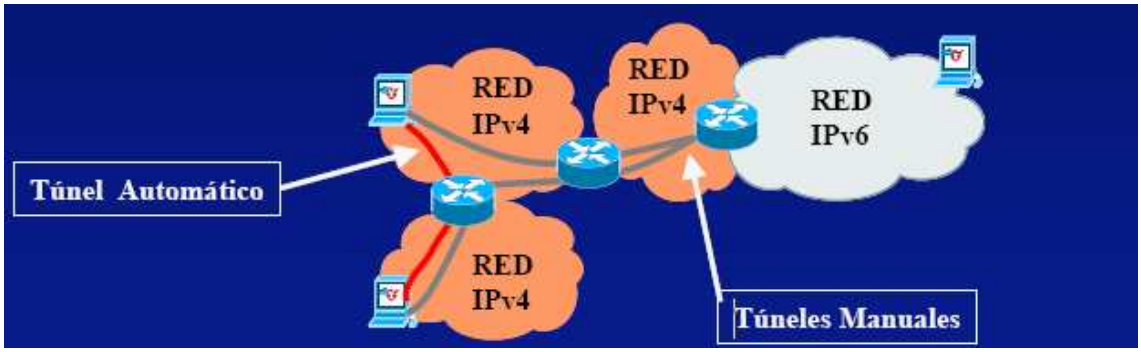


Figura 4.8 Uso de túneles manuales y automáticos [44]

Ventajas

Los túneles se establecen de manera automática, cuando se lo requiera.

4.1.2.3 Túneles 6to4

Características Principales:

- Unir islas IPv6 dispersas en un océano IPv4.
- A cada isla IPv6 se le asigna un prefijo IPv6 2002::/16 + Dirección IP del enrutador frontera.
- Siguiente salto IPv4 contenido en la dirección IPv6.
- El encaminamiento en las distintas islas se apoya en el encaminamiento IPv4 subyacente.

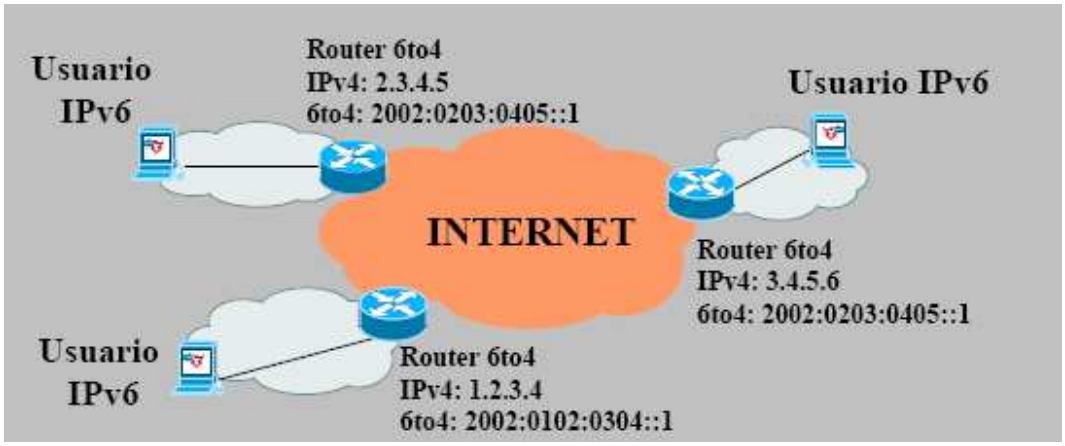


Figura 4.9 Túnel 6to4 [44]

Ventajas

- Al igual que los túneles manuales son transparentes a nivel IPv6 y por tanto no afectan a las aplicaciones.
- Se tratan de túneles establecidos dinámicamente y sin configuración previa.
- Dadas N islas solo se establecen los túneles necesarios para las conexiones activas en cada momento.

4.1.2.4 6 over 4

Una tecnología IPv6 diseñada para favorecer la coexistencia con IPv4, que proporciona conectividad *unicast* y *multicast* a través de una infraestructura IPv4 con soporte para *multicast*, empleando la red IPv4 como un enlace lógico *multicast*.

Características Principales :

- Nodos IPv6 dispersos en subredes IPv4. Se forma una LAN virtual IPv6.
- Tráfico IPv6 entre nodos encapsulados en IPv4. Direcciones IPv4 *multicast.*

- Los procesos de *Neighbor/Router Discovery* se hacen empleando *multicast*.

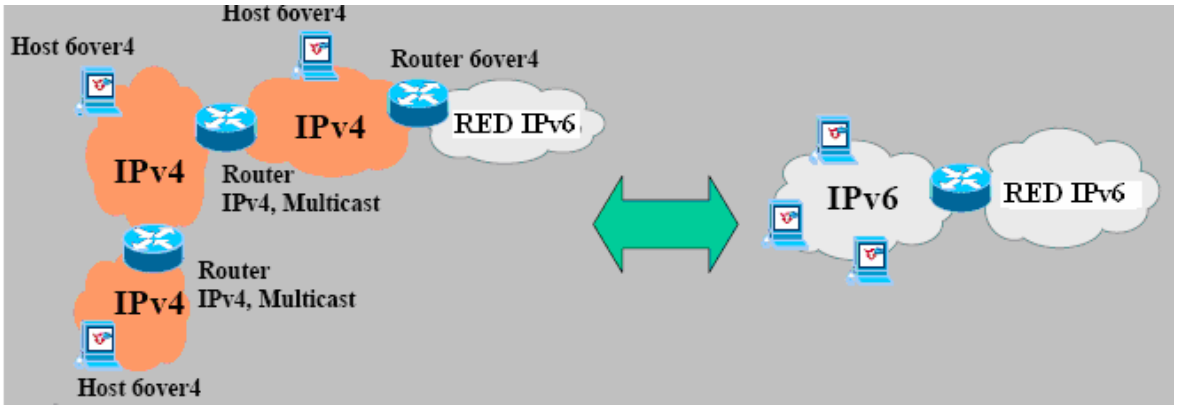


Figura 4.10 Túnel 6over4 [44]

Ventajas

- Al igual que los túneles anteriores son transparentes a nivel IPv6 y por tanto no afectan a las aplicaciones.
- Se trata de túneles establecidos dinámicamente y sin configuración previa.
- Instalando en solo enrutador el *stack* IPv6 y conectándolo a la red IPv6 se proporciona acceso a dicha red al todo el resto de nodos.

4.1.2.5 NAT-PT (*Network Address Translation - Protocol Translation*)

Características Principales

- NAT Tradicional: Traduce direcciones (conexión de redes con dirección IPv4 privado).
- NAT-PT: Traducción de direcciones y protocolo.
- Traducción basada en el Algoritmo de Transición *Stateless* (SIIT).
- No es transparente a nivel de aplicación.

- DNS-ALG: Transforma peticiones DNS (*Domain Name Server*) “A” a peticiones “AAAA”.
- FTP-ALG: Las conexiones con FTP (*File Transfer Protocol*) son problemáticas pues abren dos conexiones TCP intercambiando direcciones IP a nivel de aplicación.

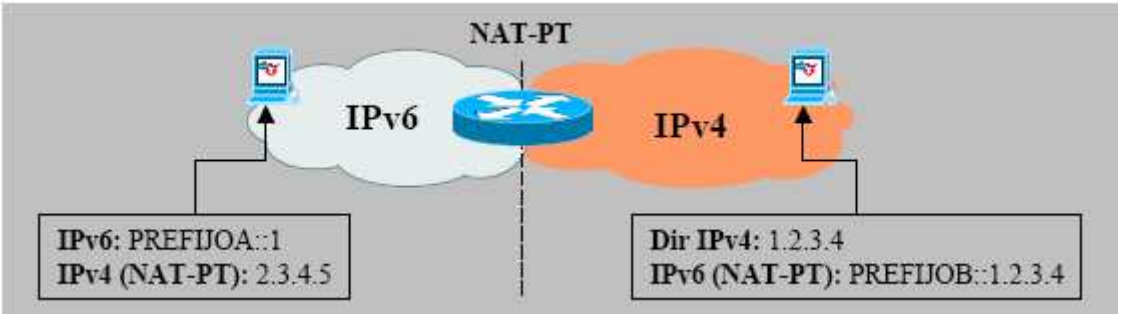


Figura 4.11 Túnel NAT PT [44]

Ventajas

- Se posee mucha experiencia en la administración y gestión de NATs.
- Implementado en la mayor parte de enrutadores (Cisco, GNU/Linux) y en algunas plataformas habituales en nodos finales (Windows, GNU/Linux).
- Si la comunicación extremo a extremo es heterogénea (IPvX IPvY) NAT- PT resulta adecuado.

Desventajas

- El proceso de traducción es más costoso en recursos que el de hacer túneles.
- Si en un protocolo de aplicación intercambian direcciones IP (DNS FTP, etc.), es necesario una extensión o módulo que incluya un algoritmo para su tratamiento específico (DNS-ALG, FTP-ALG).

4.1.2.6 SOCKSv5

Características principales

- Uso tradicional *SOCKSv5*: conectividad directa a Internet en redes con *firewall* a determinados *host*.
- Servidor *SOCKSv5* dual (Traductor de protocolos).
- Traducción IPv4-IPv6 y viceversa. Conexiones siempre iniciadas por el cliente.
- Dos componentes: Servidor *SOCKSv5* + Librería *SOCKSv5* (cliente).

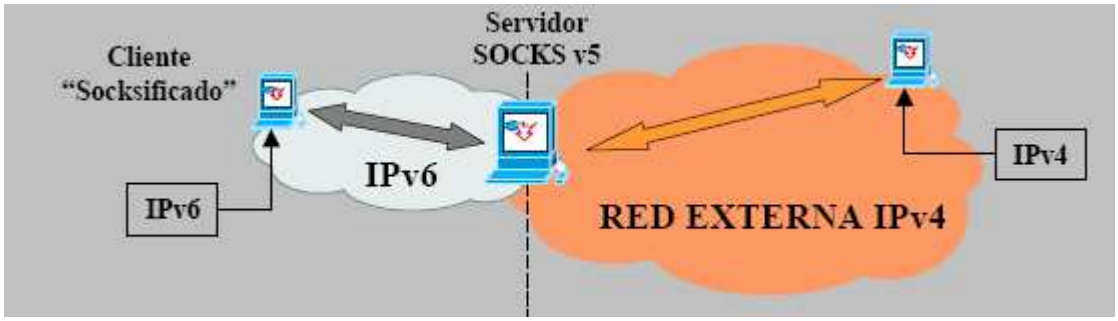


Figura 4.12 Túnel SOCKSv5 [44]

Ventajas

- Sistema apto para usuarios que deseen dar acceso a determinados nodos internos a servicios IPv6 sin probar exhaustivamente el protocolo.
- Provee sistemas de autenticación adecuados para evitar usos indeseados.

Desventajas

- Instalación de las librerías *SOCKSv5* en todos los clientes a los que se desee dar acceso.

- El factor de traducción es costoso en cuanto a consumo de recursos en el servidor, por lo que un factor limitante es la carga de tráfico prevista.
- Las conexiones solo pueden ser iniciadas por los nodos internos, con lo cual no es posible ofrecer servicios al exterior mediante este método.
- Como todos los mecanismos de traducción se debe incorporar algoritmos específicos para aquellos protocolos de aplicación que intercambien direcciones IP.

El mecanismo a utilizarse debe:

- Ser soportado por el sistema GNU/*Linux*.
- Utilizar pocos recursos computacionales.
- Ser confiable.
- Ser transparente a las aplicaciones.
- Fácil de administrar e implementar.

Bajo esta perspectiva los túneles que se adaptan a las necesidades y a la realidad son los túneles manuales, ya que no se depende de direcciones compatibles, además el número de miembros de CEDIA no es elevado y sus proyecciones de crecimiento tampoco lo son.

Para el caso que el número de miembros crezca repentinamente y las necesidades de interconexión entre los miembros a través del Internet comercial sean muy frecuentes, se recomienda la utilización de túneles automáticos.

4.1.3 DIAGRAMA DEL SISTEMA

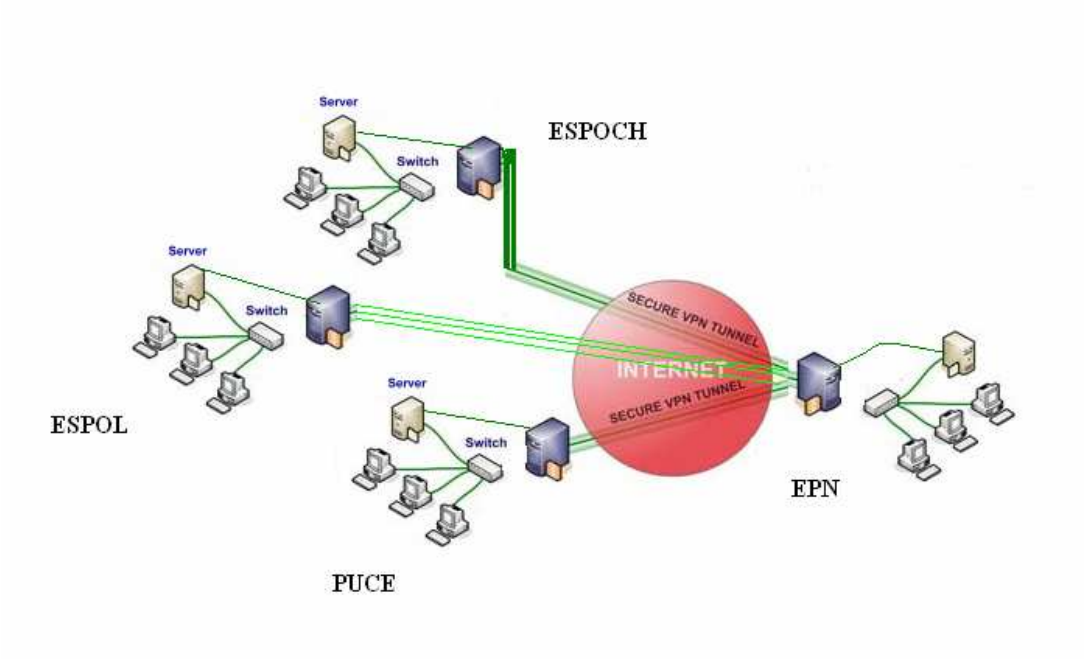


Figura 4.13 Sistema de Comunicación entre los miembros de CEDIA

Se propone esta nueva topología:

Las PCs están conectadas a un *switch*.

El *switch* tiene una conexión a un equipo GNU/*Linux*, el mismo que realizará las siguientes funciones:

- Encriptar la información.
- Establecer el túnel IPv6/IPv4

El siguiente salto es el enrutador de acceso a Internet, al cual el equipo GNU/Linux se conecta.

Para el enrutador de acceso así como para los enrutadores de Internet el tráfico es transparente pues el túnel lo hace el GNU/Linux.

A continuación se explica el proceso que se necesita cuando desee utilizar este sistema:

Se debe establecer un nodo IPv6/IPv4

Leyes de IP dual

El mecanismo para que IPv4 e IPv6 coexistan, es que el *stack* de ambos protocolos sean implementados en un mismo dispositivo (enrutador, PC o servidor), el cual está referido como un nodo IPv6/IPv4. En este caso el equipo con GNU/Linux será el nodo IPv6/IPv4.

El nodo IPv6/IPv4 tiene la capacidad de enviar y recibir ambos tipos de paquetes IPv4 e IPv6 y puede ínter operar con un dispositivo IPv4 usando paquetes IPv4 y con un dispositivo IPv6 usando paquetes IPv6.

El nodo ínteropera con las PCs de los clientes que utilizan IPv6, y con el enrutador de acceso que entiende IPv4.

El Nodo IPv6/IPv4 puede ser configurado con direcciones soportadas en ambos protocolos, estas direcciones se pueden configurar manualmente o a través de un protocolo de configuración dinámica (DHCP), conjuntamente con un protocolo de inicio (BOOTP) y el sistema de nombre de dominio (DNS), los cuales deben ser involucrados en este proceso.

Seguridad del enlace

El protocolo IPv6 establece la utilización de IPsec para seguridad de los datos. Por consiguiente se utilizará este protocolo.

Encapsulamiento

Encapsulamiento es el proceso por el cual la información de un protocolo es encapsulado dentro de otro, en este caso IPv6 será encapsulado en IPv4.

Del proceso de encapsulamiento resulta un paquete IPv4 que contiene ambos encabezados el de IPv6 y el de IPv4. El encapsulamiento incluye tres pasos:

- Encapsulamiento,
- Desencapsulamiento y
- Manejo del túnel.

En el nodo encapsulador (emisor o punto de entrada del túnel) el encabezado IPv4 es creado y encapsulado el paquete a transmitir, en el nodo desencapsulador (Receptor o salida del Túnel) el encabezado IPv4 es removido y el paquete IPv6 es procesado. En adición el nodo encapsulador puede mantener la información de configuración considerando el túnel establecido con un máximo tamaño de unidad de referencia soportada por el Túnel (MTU).

Existen cuatro posibles configuraciones de túneles que pueden ser establecidos entre enrutadores y equipos: [45]

***1. Routers* a *Routers*:** Enrutadores IPv6/IPv4 que están separados por una infraestructura IPv4 con un túnel IPv6 entre ellos mismos, en este caso el túnel puede ser colocado sobre un segmento del camino *end to end* del paquete.

***2. Host* a *Router*:** Un *Host* IPv6/IPv4 hace un túnel de un paquete IPv6 hacia un enrutador IPv6/IPv4 el cual es alcanzable por una infraestructura IPv4, en este caso el túnel se puede colocar en el primer segmento del camino *end to end* del paquete.

***3. Host* a *Host*:** Un *Host* IPv6/IPv4 que está interconectado por una infraestructura puede hacer un túnel del paquete IPv6 a través de la infraestructura IPv4 en este caso, el túnel se coloca en el camino entero *end to end* del paquete.

***4. Router* a *Host*:** Un enrutador IPv6/IPv4 puede entregar paquetes IPv6 para un equipo IPv6/IPv4 el cual es el destino final. En este el caso el túnel se deberá colocar al final del segmento del camino *end to end* del paquete.

Para que un túnel esté operativo, las direcciones de ambos extremos del túnel y los destinos del paquete deben ser conocidos y estas dos direcciones no necesariamente son las mismas, la manera en la cual la dirección al final del túnel es determinada define los tipos de túneles, que pueden ser automáticos o configurados.

El túnel automático se establecerá cuando la dirección de los nodos (IPv6) sea una dirección IPv4 compatible, caso contrario se debe cargar un archivo de configuración para establecer el túnel manualmente.

Bajo estos esquemas se estaría dando la posibilidad de que las *Intranets* de los miembros se interconecten entre sí a través de Internet de manera segura, confiable y aprovechando las ventajas de utilizar IPv6.

Se sugiere entonces que en las PCs sea habilitado el protocolo IPv6.

En este proceso se establecerá un túnel:

- ***Router to Router***

  Es el enlace que establecerá el NODO IPv6/IPv4 (equipo con GNU/Linux) con su similar en otro campus.

Figura 4.14 Túnel *router to router* [45]

4.1.4 IMPLEMENTACIÓN EN EL SISTEMA GNU/LINUX [43]

4.1.4.1 Configuración IPv6

Se necesita configurar el sistema:

Hacer clic en inicio, Configuración del Sistema, Configuración de Red y a continuación clic en Dispositivo de Red. O abrimos un terminal y digitamos *system-config-network.*

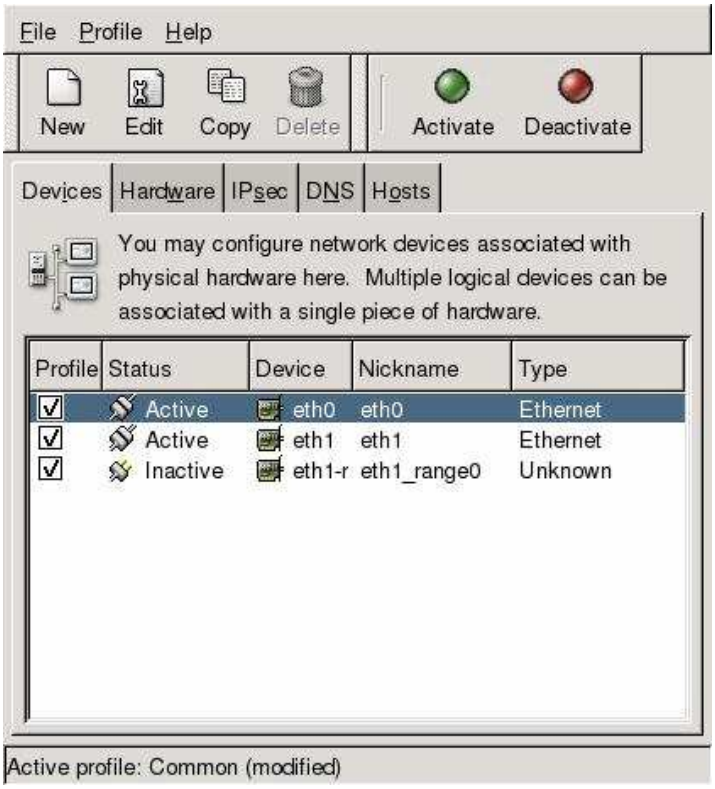


Figura 4.15 Ventana de configuración de interfaces de red GNU/*Linux* [43]

Se configura la dirección IP del equipo local y la máscara de subred.

Se necesita cargar el módulo IPv6, para esto se debe editar varios archivos:

Buscar el archivo: *etc/sysconfig/network*

Se cambia el valor de NETWORKING_IPV6 a **yes**

NETWORKING_IPV6=yes

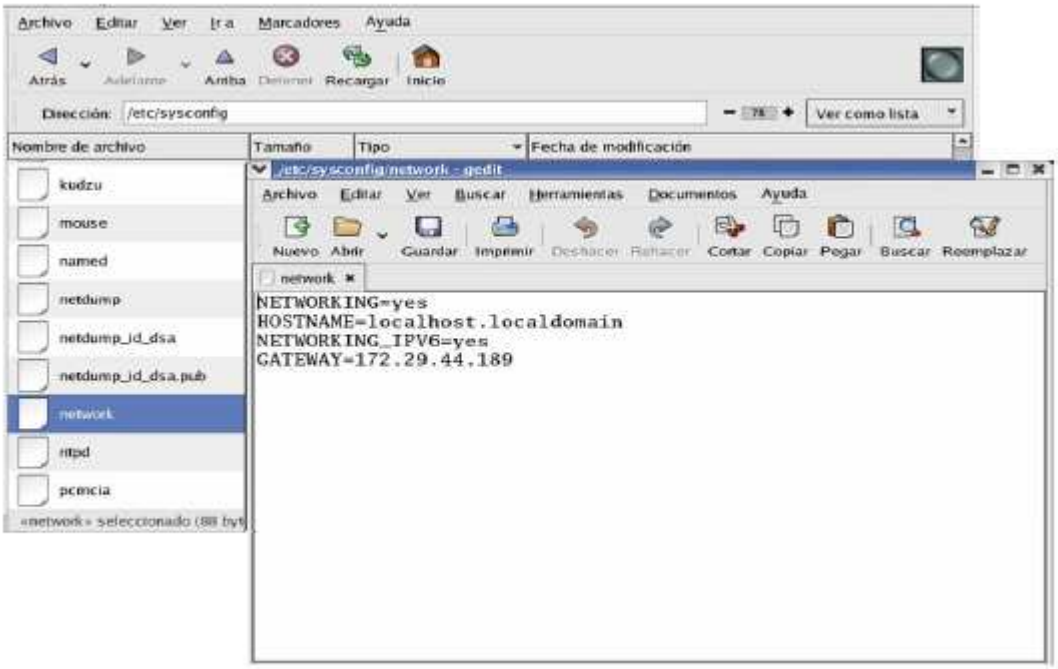


Figura 4.16 Archivo *etc/sysconfig/network* [43]

Con esto ya se ha habilitado el soporte del protocolo.

4.1.4.2 Configuración del enrutador

Se debe modificar el archivo de configuración de la interfaz Ethernet deseada.

El equipo tiene dos interfaces, eth0 y eth1.

eth0: está configurada para que soporte IPv4 e IPv6.

eth1: está configurada para que soporte IPv6.

Se utiliza la interfaz eth0 para esto se busca el archivo de configuración:

etc/sysconfig/network-scripts/ifcfg-eth0

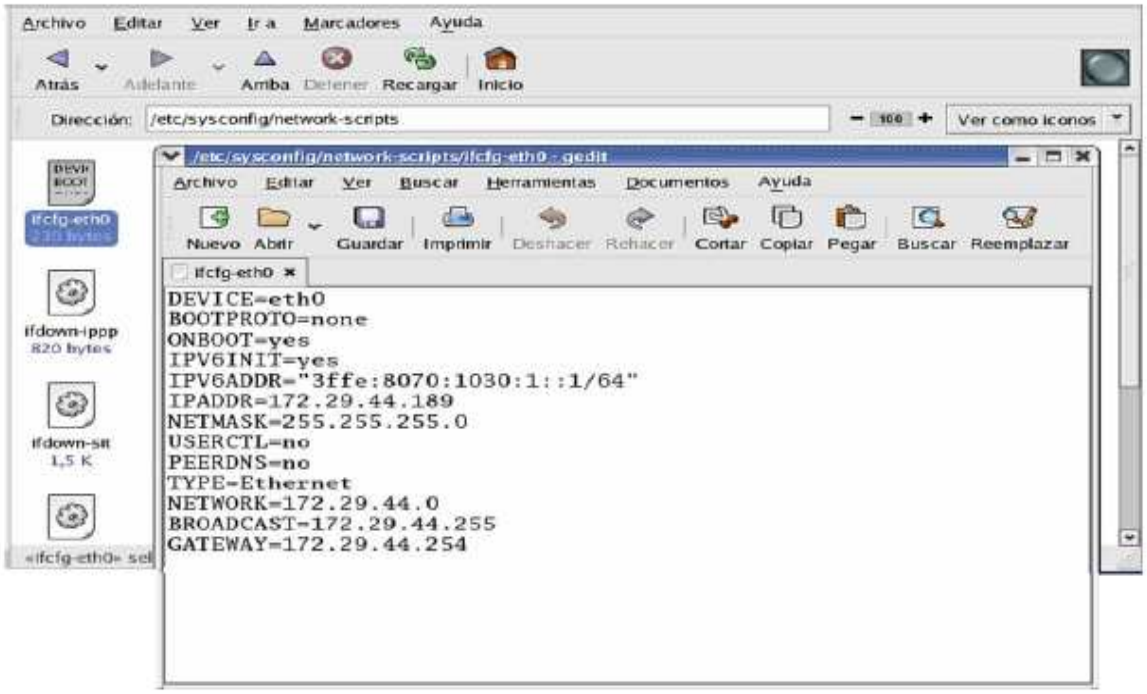


Figura 4.17 Archivo de configuración de la interfaz de red [43]

A este archivo se le añade la línea:

IPV6INIT="yes"

Para habilitar la configuración IPv6 en esta interfaz.

Ahora se asigna una dirección IPv6 a la interfaz de red.

IPV6ADDR="3ffe:8070:1026:1::1/64 " (Dirección de ejemplo)

En esta variable se configura la dirección asignada correspondiente a cada nodo.

En el equipo remoto se coloca la dirección correspondiente que le haya sido asignada por ejemplo "3ffe:8070:1026:1::2/64".

Una vez hecho esto se guardan los cambios, y es necesario reiniciar el demonio *network* para hacer efectivos todos los cambios, para esto se digita en consola el comando:

/etc/init.d/network restart

ó

service network restart

Ya se está en condiciones de utilizar el protocolo.

A continuación se comprueba que los cambios se efectuaron con éxito, se digita el comando *ifconfig.*

Se debe comprobar que existe comunicación IPv6 entre ambos equipos para lo cual se usa el comando ping. Para hacer un ping IPv6 es necesario disponer del comando ping6.

4.1.4.3 Configuración y Prueba de IPSec para IPv6

Se trata de un *software* de libre distribución, muchas de las distribuciones de GNU/LINUX, como Red Hat, SUSE o MANDRAKE incluyen paquetes rpm para su instalación.

Básicamente, está formado por:

- **KLIPS (*kernel* IPsec).** Se trata de la implementación de los protocolos AH y ESP y se encarga, también, de la gestión de datagramas dentro del *kernel* del sistema.

- **Pluto.** Es el demonio del protocolo IKE (Internet Key Exchange), se encarga de negociar las conexiones con otros sistemas.

- Varios *scrpits* que proporcionan al administrador, una interfaz con los protocolos IPSec.

Para implementar IPSec vamos a utilizar un software de libre distribución llamado Frees/wan

Instalación de Frees/wan

1. Para llevar a cabo la instalación de Frees/wan se necesita que los equipos con GNU/Linux se puedan conectar a Internet. Esta instalación se la debe realizar en todos los equipos GNU/Linux, los cuales estarán en cada miembro de CEDIA para establecer los túneles.

2. Descargar el archivo de instalación de Frees/wan. (Escoger el sistema operativo en el cual se va a instalar Frees/wan).

   - Frees/WAN se puede instalar sobre cualquiera de los siguientes *Kernels* 2.0.3X, 2.2.1X o 2.4.X. Para comprobar la versión del *kernel* del equipo se digita en la consola el siguiente comando:

     # uname –r

   - Según la versión del *kernel* se debe descargar el módulo compatible.
   - Descargar el módulo compatible con el *kernel*.

- Descargar las utilidades de Frees/wan
- Instalar los paquetes descargados.

Una vez instaldos todos los paquetes de Frees/wan se procede a la configuración del protocolo IPSec.

Para comprobar que la instalación y la configuración han sido correctas se ejecuta *ifconfig* y se observa que aparece una interfaz virtual como se muestra en la figura 4.17

4.1.4.4 Creación de Túneles IPv6 en IPv4 en *Red Hat* GNU/*Linux*

Para poder manejar tráfico IPv6 en redes separadas por enrutadores IPv4 se debe recurrir a los túneles. A través de ellos se envían los paquetes IPv6 encapsulados en paquetes IPv4 hacia otra red que maneje también el protocolo.

Con esto se logra unir nubes IPv6, pero introducidos en redes del tipo IPv4. Antes de la creación de los túneles se necesitan varios datos:

- Dirección IPv4 del enrutador: Ejemplo: 172.29.44.188
- Dirección IPv4 del enrutador remoto. Ejemplo: 172.29.44.189
- Dirección IPv6 para el túnel:

  Ejemplo:

  3ffe:8070:1026:1::1/64 para el equipo local.

  3ffe:8070:1026:1::2/64 para el equipo remoto.

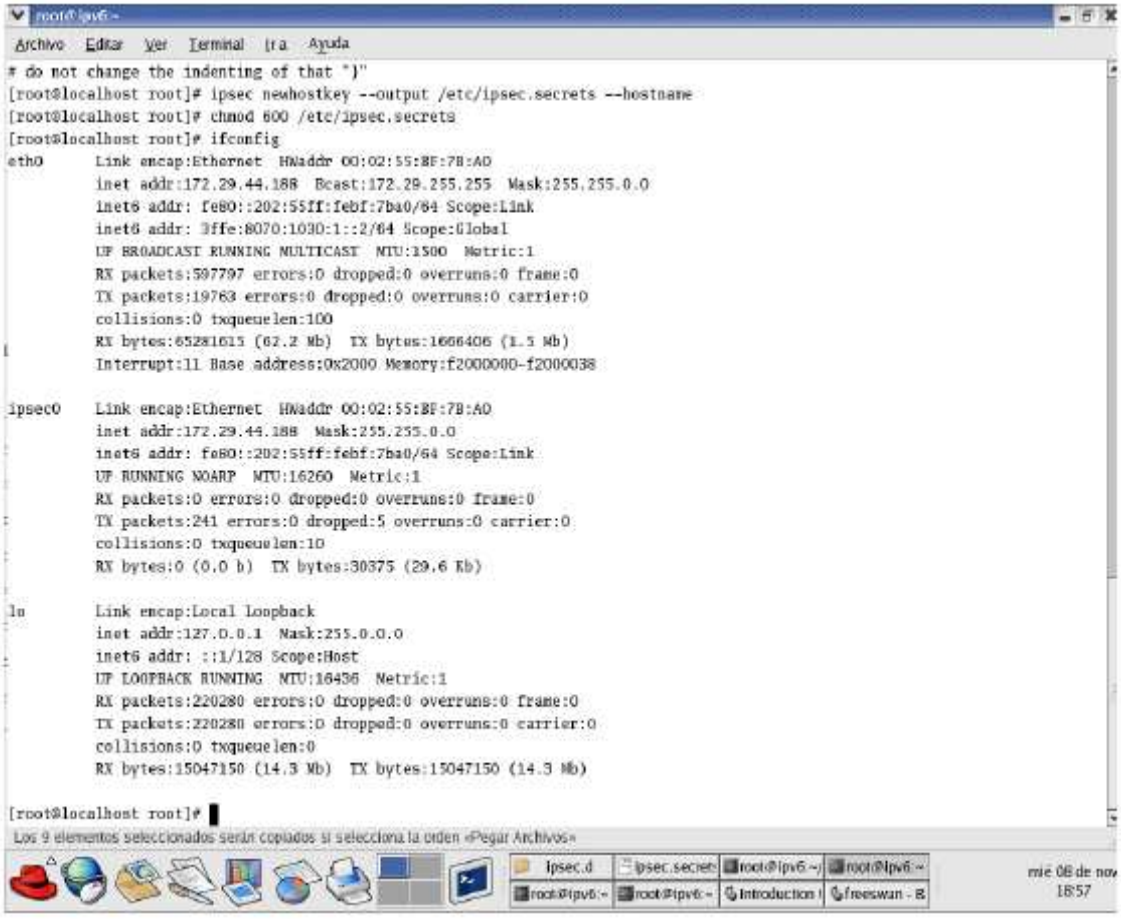


Figura 4.18 Nueva interfaz creada para IPSec

Ubicar los archivos: /etc/sysconfig/networkscripts/

GNU/Linux permite tener interfaces con un nombre distintivo y que se inician cuando se activa el sistema. Se escoge el archivo ifcfg-eth0 y a este se le realizan algunas modificaciones:

Crear el archivo ifcfg-<nombre> para el ejemplo el nombre del archivo es túnel.

Ejemplo del contenido del archivo:

DEVICE=tunel
BOOTPROTO=none

ONBOOT=yes
IPV6INIT=yes
IPV6TUNNELIPV4=172.29.44.188
IPV6ADDR=3ffe:8070:1026:1::1/64
IPV6_DEFAULTGW=3ffe:8070:1026:1::2/64
IPV6_DEFAULTDEV=tunnel

En este archivo se especifican la dirección IPv4 remota, el extremo del túnel, el *gateway*.

Ejecutar los siguientes comandos en consola:

ln -s ifup-sit ifup-tunel

ln -s ifdown-sit ifdown-tunel

Con esto se crea un enlace simbólico hacia los archivos donde están las funciones necesarias para subir y bajar el túnel.

Se debe reiniciar el *network configuration*

/etc/init.d/network restart

Con esto, ya se tiene un túnel cuyo nombre será tunel.

Al digitar el comando *ifconfig* se observará el dispositivo del túnel:

tunel Link encap:IPv6-in-IPv4
inet6 addr: 3ffe:8070:1026:1::1/64 Scope:Global
inet6 addr: 3ffe:8070:1026:1::2/64 Scope:Link
UP POINTOPOINT RUNNING NOARP MTU:1480 Metric:1

RX packets:692080 errors:0 dropped:0 overruns:0 frame:0
TX packets:692944 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:113649875 (108.3 Mb) TX bytes:60870452 (58.0 Mb)

Opcionalmente se puede activar el túnel ejecutando simplemente:

Para Activar: ifup <nombre>

Ejemplo:

Ifup tunel

Para Desactivar: ifdown <nombre>

Ejemplo:

Ifdown tunel

4.1.5 MULTICAST

Para tener una mayor eficiencia y ahorro de recursos durante la ejecución de las aplicaciones de las redes avanzadas, especialmente las videoconferencias es necesario utilizar la tecnología *multicast*.

Para establecer conectividad *multicast* con otras máquinas o redes es necesario unirse a las redes experimentales MBone ó M6Bone, puesto que, si sólo uno de los enrutadores entre ellos no soporta *multicast*, los paquetes son simplemente descartados y jamás llegarán a su destino, éste es el caso que tenemos con el Internet de la actualidad.

Se aprovechará la ventaja de tener asignado un bloque de direcciones IPv6 para obtener esta funcionalidad, puesto que, al utilizar IPv6 garantizamos el soporte de direcciones *multicast*.

Las direcciones *multicast* en IPv6 identifican un grupo de interfaces, un paquete destinado a una dirección *multicast* llega a todas las interfaces que se encuentran agrupadas bajo dicha dirección.

Dirección IPv6	Longitud del Prefijo (Bits)	Descripción
ff:0000:0000:0000:0000:0000:0000:0000	8 bits	*multicast*

Para el uso de la tecnología *multicast* con direcciones IPv6 es necesario unirnos a la red M6Bone.

4.1.5.1 M6Bone

La figura 4.10 nos muestra la cobertura mundial de la red M6Bone.

M6Bone es administrada por la Red Francesa de Investigación y Desarrollo RENATER, como se observa, a esta red se conectan principalmente redes académicas y de investigación, sin embargo, cualquier conexión al Internet comercial permite unirse a ella.

En América Latina la Universidad de Guadalajara en México es el punto de contacto, en la Universidad Austral de Chile se encuentra el nodo IPv6 *multicast*.

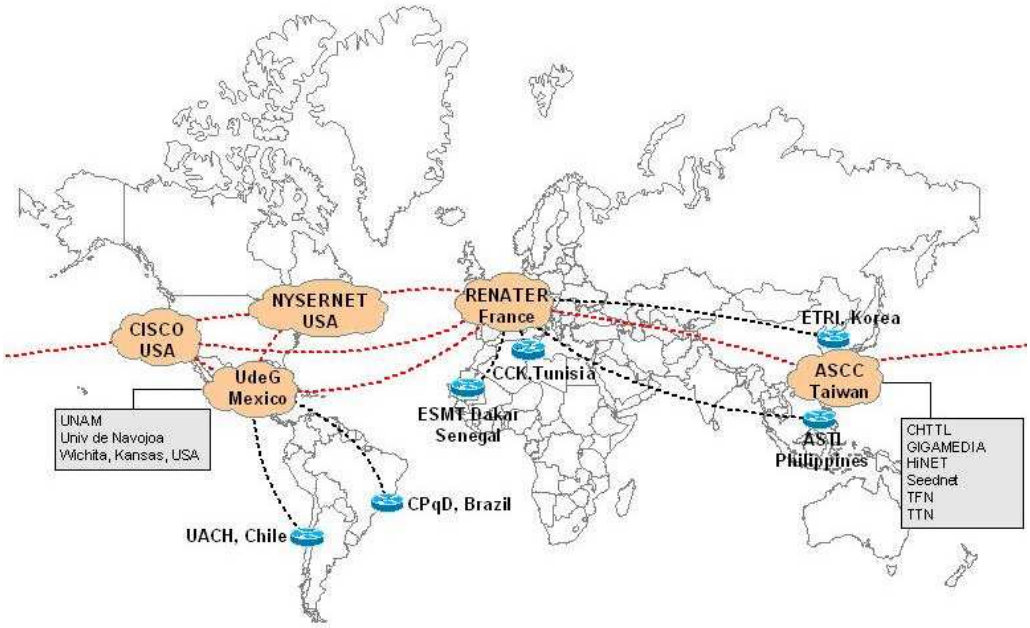


Figura 4.19 Red M6Bone [46]

Acceso a M6Bone

Para conectarse a la red M6Bone a través del Internet comercial y así poder cursar tráfico *multicast* se deben cumplir con los siguientes requisitos:

Pertenecer a lista de correo m6bone@ml.renater.fr, la suscripción se la realiza a través de la dirección https://listes.renater.fr/sympa, luego de recibir el mail de suscripción, es necesario enviar un formulario con nuestros datos a la dirección de correo sympa@ml.renater.fr, el moderador de la lista remitirá un mensaje delegando las direcciones que se han otorgado para establecer el túnel de conexión hacia M6Bone.

Mostramos un ejemplo de cómo debería ser llenado el formulario:

```
> * Site
>   - Name: Escuela Politécnica Nacional
>   - Address:QUITO-ECUADOR
>
> * Technical contact 1
>   - Name:DIANA MARTINEZ
>   - Phone Number:59395400687
>   - Email Address:diana.martinez@interactive.com.ec
>
> * Technical contact 2
>   - Name:LUIS MACHADO
>   - Phone Number:59396192803
>   - Email Address:luis_fem@yahoo.es
>
> * Routing information
>   - IPv6 prefix of your site:2800:68
>   - AS number (mention "static" if static routing):
     2800:68.:0011::/48
>
> * Tunnel configuration
>   - Tunnel mode (IPv6/IPv6, IPv6/IPv4, GRE...):IPv6/IPv4
>   - Tunnel end-point
>         . IPv6 address if IPv6 in IPv6 tunnel:no
>         . IPv4 address if IPv6 in IPv4 tunnel:yes
```

El túnel a ser establecido será IPv6 en IPv4, ya que los equipos de frontera no soportan IPv6 nativo.

Si se desea poseer una estructura SSM (*Source Specific Multicast*), donde el grupo recibirá datos de una fuente específica, se debe:

- Primeramente asegurar que el servicio de *multicast* esté habilitado en la red local.
- Habilitar el protocolo PIM-SMv2 (*Protocol Independent Multicast-Sparse Mode version 2*) para el transporte y enrutamiento del tráfico *multicast*, en todos los equipos de enrutamiento de la red local.
- Usar la tabla de enrutamiento *multicast* de BGP.

- Conocer el prefijo *multicast* IPv6.
- Poseer un equipo configurado para el establecimiento del túnel hacia un enrutador dedicado M6Bone.

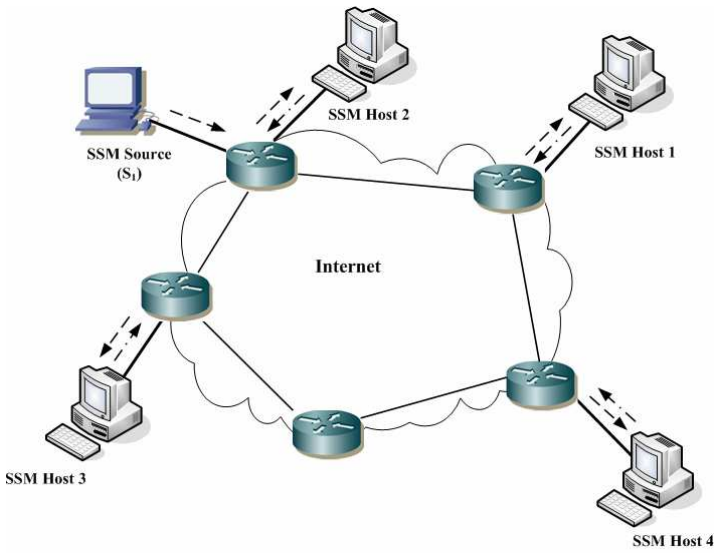


Figura 4.20 Comunicación *multicast* con SSM

Si se desea tener una estructura ASM (*Any Source Multicast*), donde el grupo recibirá información de cualquier fuente, se debe cumplir adicionalmente con lo siguiente:

- Asegurarse de la habilitación del *embedded*-RP en los ruteadores de la red local, es decir, según lo especifica el RFC 3956, la dirección del *Redezvous Point* (RP) deberá ser embebida en una dirección *multicast* IPv6.

  Un Redezvous Point es punto de encuentro, es un enrutador especificado en las implementaciones PIM, para tener registro de los miembros de

grupos *multicast* (emisores y receptores) y entregar los mensajes a las direcciones conocidas de los grupos.

- Configurar la herramienta de monitoreo DBeacon la cual permite recopilar información estadística acerca de pérdidas de datos, retardos o variaciones de la señal (*jitter*).

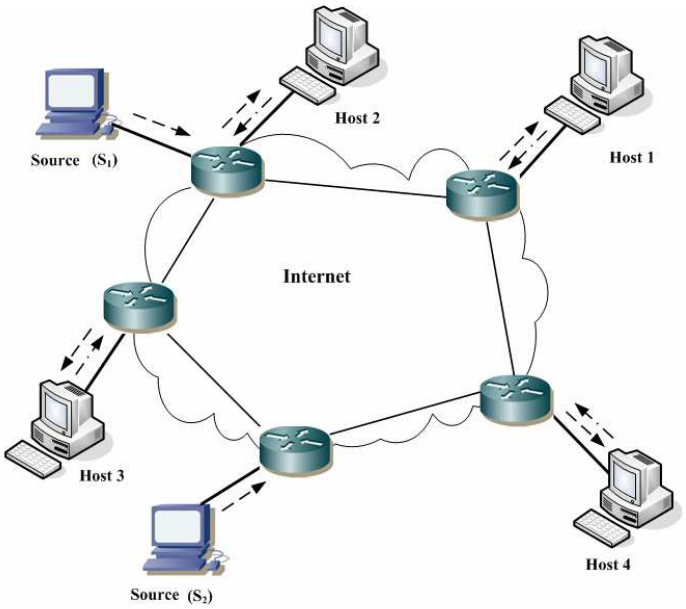


Figura 4.21 Comunicación *multicast* ASM

4.1.5.2 Configuración de equipos

A continuación describiremos los pasos a seguirse para la configuración de los equipos para el acceso a M6Bone con la estructura SSM.

- **Habilitar servicio *multicast* en la red local**

  Debido a que la solución que se propone, en cuanto a equipos de enrutamiento, se basa en el sistema operativo GNU/Linux, primeramente

se describirá los pasos para la configuración del enrutador para el soporte *multicast*.

Se tiene la ventaja que el núcleo de GNU/Linux tiene soporte nativo de *multicast* y soporta el protocolo IGMPv2 (*Internet Group Management Protocol version 2*).

El protocolo de red IGMP se utiliza para intercambiar información acerca de quienes admiten *multicast* y quienes son los miembros de los grupos de *multicast* entre enrutadores IP.

En GNU/Linux se pueden definir rutas *multicast* que le indican al núcleo que el tráfico de un grupo *multicast* específico recibido por una interfaz se tiene que encaminar directamente a otra interfaz.

Se puede consultar la información de *multicast* del núcleo con:

 # ip mroute show: muestra las rutas.

 # netstat -g o ip maddr show: muestra los grupos *multicast* asociados a una interfaz.

 # cat /proc/net/ip_mr_cache y cat /proc/net/ip_mr_vif: muestran las estadísticas de tráfico *multicast* enviado y recibido.

Para supervisar el tráfico *multicast* se puede utilizar la herramienta de captura de tráfico tcpdump:

 # tcpdump -ni eth0 igmp: muestra los paquetes IGMP recibidos en la interfaz eth0.

 # tcpdump -ni eth0 pim: muestra los paquetes PIM recibidos en la interfaz eth0.

 # tcpdump -ni eth0 ip *multicast*: muestra los paquetes IP *multicast* en la interfaz eth0.

 # tcpdump -ni eth0 ether *multicast*: muestra los paquetes Ethernet *multicast* en la interfaz eth0.

Se detallará a continuación la configuración para los equipos que se encuentran dentro de la red local para el soporte *multicast*, analizando por separado cada uno de los sistemas operativos más utilizados.

FreeBSD

Las operaciones *multicast* están totalmente soportadas en FreeBSD a partir de la versión 2.0.

Windows XP

1. Necesita tener instalado el Service Pack 1 o posterior.
2. También se requiere tener instalado el stack de IPv6.

Nota: El software debe ser completamente legal. Es necesario depurar las direcciones que sean anónimas de la estación, para esto se realizan los siguientes pasos:

1.- Abrir una ventana de comando.

2.- Teclear lo siguiente:

c:\windows\>IPv6 –p gpu UseAnonymousAddressess no

De esta manera lograremos quitar las direcciones que sean anónimas.

- **Habilitación del protocolo PIM-SMv2.**

  Se recomienda el uso de la aplicación Xorp, la cual implementa distintos mecanismos de enrutamiento, soporta en la actualidad los protocolos de enrutamiento dinámico OSPF (*Open Shortest Path First*), BGP (*Border Gateway Protocol*), RIP (*Routing Information Protocol*) y los protocolos de *multicast* IGMP (versión 2) y PIM-SM.

Para monitorizar el estado del enrutador se utiliza el siguiente comando:

xorpsh

Al ejecutarlo se ingresará a un indicador en el que se pueden ejecutar, entre otros, estos comandos:

 # show igmp group: Muestra la lista de los grupos *multicast* y las interfaces asociadas.

 # show pim interface: Muestra la lista de las interfaces y el enrutador principal (DR, *Designated Router*) de cada red.

 # show pim neighbors: Muestra los enrutadores *multicast* adyacentes.

 # show pim rps: Muestra los enrutadores principales para el sistema

.

 # show pim join: Muestra los grupos *multicast* negociados por PIM.

 # show pim mfc: Muestra las rutas *multicast* definidas

- **Tabla de enrutamiento *multicast* de BGP.**

  A través del uso de la aplicación Xorp, garantizamos el soporte del protocolo BGP.

- **Prefijo *multicast* IPv6**

  Se conoce el prefijo *multicast* IPv6 de los miembros de CEDIA, el prefijo es 2800:68.

- **Túnel a M6Bone**

  Ya se posee un equipo dedicado para el establecimiento del túnel hacia un enrutador dedicado M6Bone, éste además debe estar configurado de modo que la interfaz de salida hacia Internet tenga una sub-interfaz con una dirección ip pública la cual será habilitada el momento de la pérdida de conexión con la red avanzada ecuatoriana y mediante el algoritmo cbq (Class-Based Queuing), el cual viene instalado en el *kernel* de GNU/Linux a través del paquete iproute-2 se limitará a utilizar el 50% del total de la capacidad del enlace hacia Internet.

Para el caso de la limitación del ancho de banda mediante cbq, se deberá seguir el siguiente procedimiento:

- En el archivo /etc/sysconfig/cbq se deberá crear un archivo por cada regla de limitación.

- Cada archivo deberá ser nombrado según el formato:

  cbq-<clsid>.<name>

  Donde:

  <clsid> es un número hexadecimal de dos bytes dentro del rango <0002-FFFF>

  <name> es el nombre de la regla.

- En cada archivo de configuración deberá constar la siguiente información:

  DEVICE= (int-nombre),(banda),(peso)
  RATE= (velocidad)
  WEITH= (velocidad/10)
  PRIO= (prioridad)
  RULE= (ip o red a ser controlada)

  - Parámetro DEVICE, (Obligatorio)

    Ejemplo:
    DEVICE=eth0,10 Mbit,1 Mbit

    (int-nome) Es el nombre de la interfaz a ser controlada, por ejemplo: eth0, eth1, ppp0, wvlan0.

    (banda) Es la velocidad del dispositivo, por ejemplo: 10 Mbps o 100 Mbps.

    (peso) Es un parámetro de ajuste que debe ser proporcional a la banda, vamos a darle el 10% siempre.

- Parámetro RATE, (Obligatorio)

  Ejemplo:
  RATE=1 Mbps

  Es la capacidad que se limitará a dicha interfaz, en este caso será el 50% de la capacidad total.

- Parámetro WEIGHT, (Obligatorio)

  Ejemplo:
  WEIGHT=100 Kbps
  WEIGHT=(RATE/10)

- Parámetro PRIO, (Obligatorio)

  Ejemplo:
  PRIO=5

  Este parámetro podrá poseer un valor de 1 a 8, cuanto más elevado sea el número menor será la prioridad.

- Parámetro RULE (Obligatorio)

  Ejemplos:

  RULE=201.218.25.81:80

  Controla el tráfico de la ip 201.218.25.81 que pasa a través de la puerta
  80

  RULE=201.218.25.81

  Controla el tráfico de cualquier puerto del *host* 201.218.25.81

4.1.5.3 Aplicaciones *Multicast* [47] [48]

Al pertenecer a la red M6Bone los beneficios que se obtienen son muchos, por ejemplo el uso de herramientas de videoconferencia *multicast* como sdr,vic,rat,nte,wbd.

4.1.5.3.1 SDR (Sesion Directory)

Es una herramienta de sesión de directorio diseñada para permitir anunciar lo que los contactos están transmitiendo o están realizando y para unir conferencias de *multicast* en M6bone.

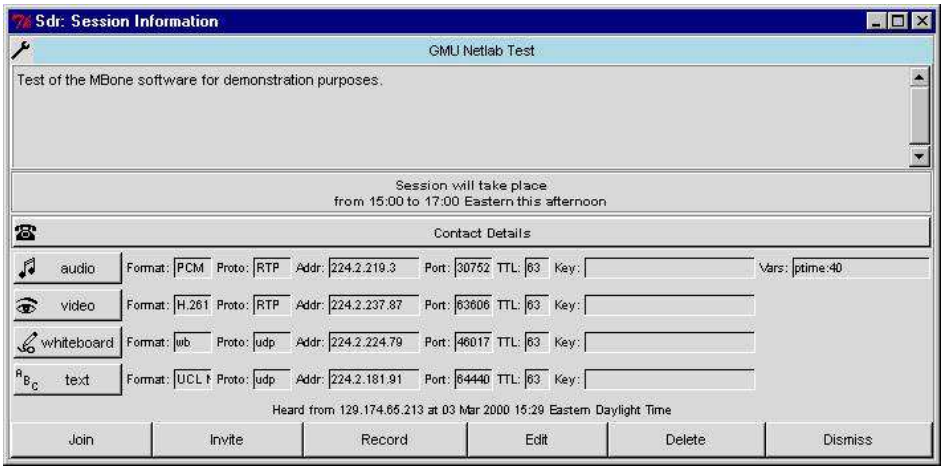
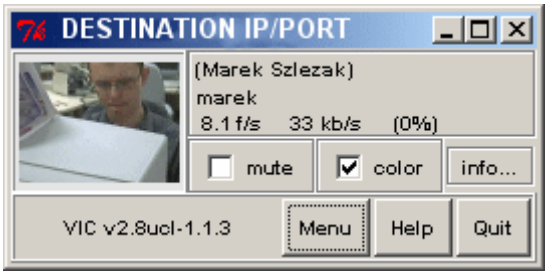


Figura 4.22 Aplicación SDR [47]

4.1.5.3.2 VIC (Video Conference)

Es una aplicación de videoconferencia desarrollado por el Grupo de Investigación de Redes del Laboratorio Nacional *Lawrence Berkeley* en colaboración con la Universidad de California.



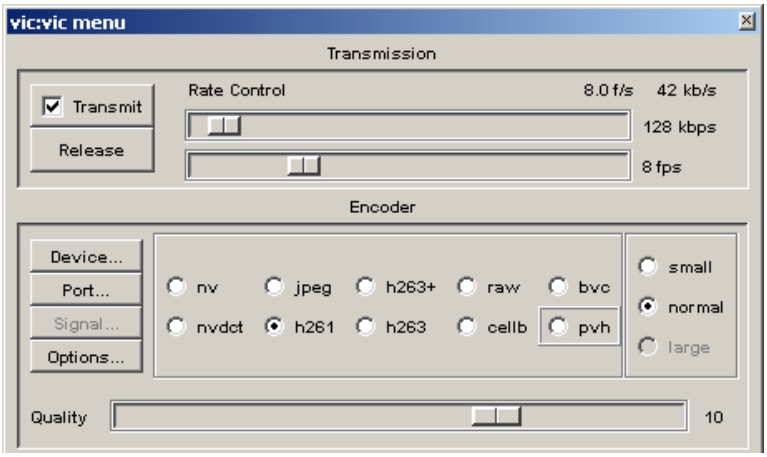


Figura 4.23 Aplicación VIC [48]

4.1.5.3.3 RAT (Robust Audio Tool)

Es una aplicación de audio-conferencia y *streaming* de código abierto que permite a los usuarios participar en audio conferencias por Internet, éstas pueden ser en parejas o entre grupos de participantes. Funciona con *multicast* sobre IPv6 o IPv4.

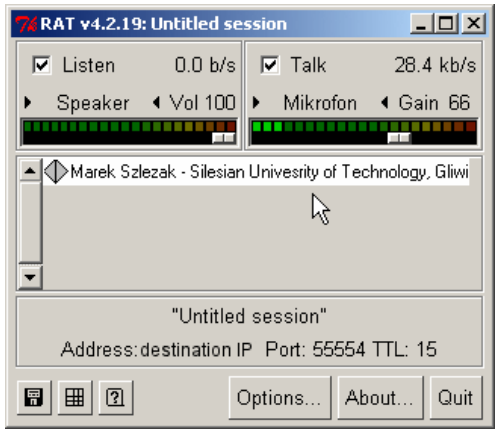


Figura 4.24 Aplicación RAT [48]

4.1.5.3.4 NTE (Network Test Editor)

Es un editor de texto compartido de uso interactivo, le permite bloquear o desbloquear el texto escrito, varias personas simultáneamente pueden usar el editor. No es procesador de palabras ni una pizarra.

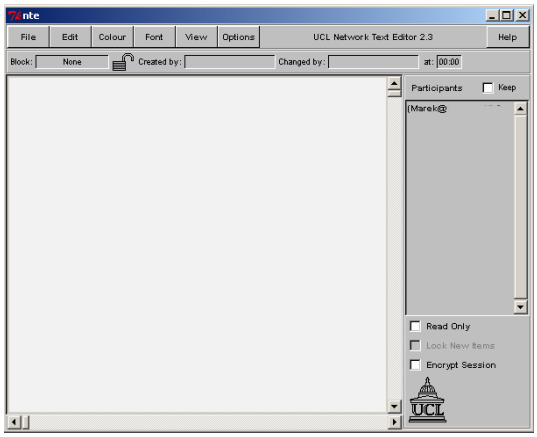


Figura 4.25 Aplicación NTE

4.1.5.3.5 WBD (White Board)

Es una pizarra compartida usando *multicast*.

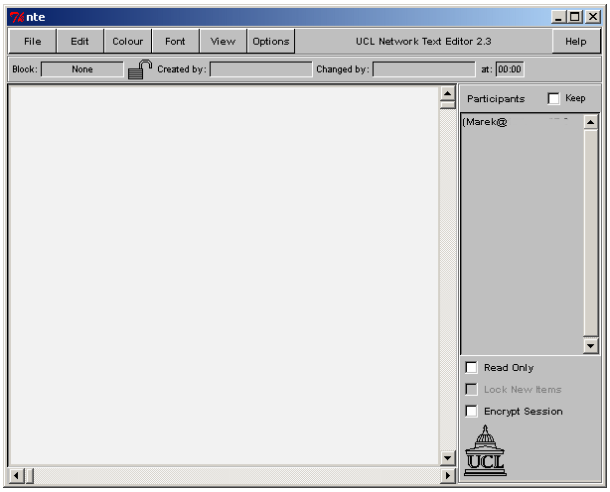


Figura 4.26 Aplicación WBD [47]

Estas aplicaciones se pueden descargar del siguiente *link*:

http://www-mice.cs.ucl.ac.uk/multimedia/software/

4.2 REQUISITOS TÉCNICOS PARA LOS NODOS PRINCIPALES

Los considerados nodos principales, aunque no poseen centralización de conexiones en la actualidad, son la Escuela Politécnica Nacional y la Escuela Politécnica del Litoral, puesto que, son las instituciones que poseen una infraestructura de red más robusta y son consideradas las más aptas para convertirse en nodos principales a futuro.

En el caso de conectarse a la red avanzada por un medio alterno, estos nodos necesitarán cumplir los mismos requisitos que los demás miembros, ya que la solución propuesta se basa en la comunicación de los miembros a través del Internet comercial, con la formación de túneles privados.

Se ha optado por esta solución, considerando que los miembros no cuentan con los suficientes recursos económicos para pagar un enlace dedicado de redundancia, como todas las instituciones tienen acceso al Internet comercial, se ha aprovechado esta ventaja para esta propuesta.

En conclusión, al establecerse el enlace a la red avanzada a través del Internet todos los miembros están en las mismas condiciones y por lo tanto los requerimientos son iguales.

4.3 REQUISITOS TÉCNICOS PARA LOS MIEMBROS DE CEDIA

Se recomienda que los miembros posean como requisitos mínimos:

- Tener contratados 2 Mbps de conexión al Internet.

- Tener asignadas 2 direcciones IP públicas, una para el Internet comercial y otra para el establecimiento del túnel.

- Poseer una máquina que será utilizada exclusivamente para enrutamiento y establecimiento de los túneles.

Características mínimas en *hardware*

- Procesador Pentium IV de 1,8GHz.
- Memoria RAM de 512 MB.
- 40 GB de Disco Duro.
- 3 Tarjetas de Red (1 para el Internet comercial, otra para la red interna IPv6 y una para la red interna IPv4).

Características mínimas en *software*

- GNU/Linux *kernel* 2.0.
- Las máquinas de los usuarios en el caso de querer hacer uso de *multicast* deberán contar con lo siguiente:
  - Contar con un dominio IPv6 (ejemplo: xpmultv6.IPv6.udg.mx).
  - Tener instaladas las herramientas de mbone, (vic,rat,sdr,nte,wbd).
  - En caso de que se tenga instalado el sistema operativo Windows, éste debe ser legal, para que en caso de que se

necesite realizar alguna actualización en el sistema no tenga ningún problema.

En el caso de desear establecer una videoconferencia, el usuario puede hacer uso de las herramientas que considere necesarias, como equipos necesarios se nombran:

- Una cámara web.

- Es recomendable utilizar una diadema con micrófono para obtener una mejor calidad en la transmisión y recepción de la voz.

4.4 PRESUPUESTO

La propuesta de los equipos prioriza el ahorro económico, estos equipos cumplen los requerimientos mínimos para el correcto funcionamiento del sistema. Sin embargo si los miembros tienen la capacidad de adquirir un equipo de última tecnología el rendimiento del sistema aumentará.

Elemento	Cantidad	Valor total
Recursos Humanos	1	$1000
Servidor para el NODO IPv6/IPv4, PENTIUM IV , 1,8 GHz de procesamiento, 1 GB RAM, 40GB en disco duro, , teclado, Mouse,	1	$1000

monitor, 3 interfaces de red		
Instalación del Servicio de Internet	1	$280
Enlace de 2048 Mbps a Internet	1	$1900
Imprevistos		$100
TOTAL		$4280

Tabla 4.1 Presupuesto para la alternativa de conexión

Esta cantidad es la que debe pagar el miembro el momento de la instalación del servicio.

Posteriormente el pago se reduce a 2900 dólares como lo muestra la tabla 4.3

Elemento	**Cantidad**	**Valor total**
Recursos Humanos	1	$1000
Enlace de 2048Mbps a Internet	1	$1900
TOTAL		$2900

Tabla 4.2 Costo mensual de mantenimiento

Cabe mencionar que los costos analizados en el presupuesto de conexión a Internet, son valores aproximados que el miembro de CEDIA ya se encuentra pagando, pero se ha considerado necesario agregarlos para quienes no posean este servicio en la actualidad.

Para finalizar, se hace énfasis que los costos están considerados sin fines de lucro, ya que en sí, la organización tiene únicamente fines educativos e investigativos.

5 CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Las redes avanzadas a nivel mundial, aunque en la actualidad están siendo utilizadas únicamente para fines educativos y de investigación, se proyectan a ser utilizadas por el público en general, ya que las comunicaciones a través de la redes de información se han vuelto una herramienta fundamental en nuestra sociedad lo que ha incrementado la demanda de nuevos servicios que superen la calidad que se posee hoy en día.

- En Ecuador se posee actualmente una red avanzada académica puesta a disposición de todos quienes tengan fines de investigación y desarrollo y no de lucro; esto nos ha permitido tener acceso a redes de mayor desempeño y poder participar en grupos de trabajo con integrantes de todas partes del mundo.

- La Comunidad Europea a través de su financiamiento para la unión de las redes avanzadas de América Latina y Europa, permitió que los países que no disponen de suficientes recursos económicos, como es el caso de Ecuador, tengan a su disposición los beneficios y ventajas que ofrece la interconexión con la tecnología de los países europeos.

- La gestión del Directorio de CEDIA a nivel nacional e internacional, ha permitido que la red avanzada mejore su rendimiento dinámicamente en provecho de todos sus miembros, como ejemplo se tienen, los convenios realizados con Telconet en cuanto al aumento de las capacidades de los enlaces, los nuevos protocolos

implementados en la Intranet que permiten un mejor rendimiento de las aplicaciones que se ejecutan entre los nodos, entre otros.

- Las Instituciones Académicas que como sistema educativo tienen fines científicos, tienen su razón de ser en nuestro medio, ya que si antes los estudios eran limitados a los recursos tecnológicos que posee el país, ahora tienen a su disposición la mayoría de beneficios que provee el mundo de la ciencia y la tecnología a través de las redes avanzadas, además de restar importancia a la ubicación geográfica.

- Proyectos como la conexión de primera milla con Transelectric, dan apertura al crecimiento de la red avanzada ecuatoriana en cuanto a velocidades de transmisión de datos, lo que representaría en cada miembro una gran ventaja para la ejecución de aquellas aplicaciones que exigen calidad de servicio y 100% de disponibilidad.

- Los talleres internacionales organizados por el Directorio de CEDIA son de gran acogida en nuestro medio puesto que a más de otras virtudes han generado plazas de pasantías en entidades educativas de otros países, como por ejemplo la Universidad de Oregon en los Estados Unidos.

- La Escuela Politécnica Nacional y la Escuela Politécnica del Litoral, luego del estudio realizado, se pueden concluir que tienen una infraestructura de red suficiente como para actuar como nodos principales de la red avanzada y unir a los demás miembros de CEDIA, ambos poseen equipamiento y personal capacitado al nivel que se requiere para este nombramiento.

- El bloque de direcciones IPv6 asignado por CLARA a CEDIA, permite que todos los miembros de la red avanzada ecuatoriana tengan la facilidad de hacer uso de todas las virtudes incorporadas en el funcionamiento del protocolo IPv6.

- En la comparación de la red CEDIA con la red REUNA claramente se distingue la gran brecha que existe entre ambas redes en cuanto a características de equipamiento, capacidades contratadas, seguridades y servicios. REUNA es una de las redes más robustas a nivel de Latinoamérica y el objetivo a seguirse desde un principio fue el imitar su evolución, igualar su funcionamiento y por qué no superarlo en un futuro.

- RNP es fruto de las grandes cantidades de recursos económicos con que cuenta Brasil, una inversión como la que ha realizado este país en su red avanzada es inalcanzable en la actualidad para el Ecuador, lo que nos lleva a la conclusión de que para tener a nuestro alcance recursos tecnológicos de gran avance, no es estrictamente necesario salirnos de la red académica establecida en América Latina.

- Luego del análisis FODA realizado para CEDIA se distingue claramente que la mayor debilidad de la organización es la falta de utilización de los recursos que tienen a su disposición todos los miembros, los cuales, estando enlazados a una red avanzada no la utilizan es su totalidad a nivel local para establecer comunicación de alta calidad entre los demás miembros y peor aun a nivel internacional.

- Otro de los problemas percibidos es la falta de apoyo gubernamental para el fortalecimiento de la Corporación. El presupuesto del Estado asignado para la educación en nuestro país no es el adecuado, lo cual, no afecta solo a estudiantes, sino, como podemos apreciar, también lo hace a proyectos de gran avance tecnológico que aportan además de al desarrollo académico a la sociedad en general.

- Las bibliotecas digitales son una fuente de información muy importante, dejaron de ser un complemento bibliográfico y se convirtieron en el primer y mejor recurso existente en la actualidad, ya que disponen de una gran cantidad de información que cubre casi en su totalidad los ámbitos de la ciencia, tecnología, cultura, música, etc.

- Las bibliotecas digitales son un aporte muy relevante para los estudiantes, nos ahorran tiempo ya que nos proveen de recursos de búsqueda inmediata, podemos encontrar los temas más diversos en poco tiempo, navegar no solo dentro de la biblioteca con el fin de encontrar el libro de nuestro interés sino profundizar la búsqueda dentro de los libros en si.

- Las bibliotecas digitales producen un ahorro económico al usuario, pues al tener la información en formato electrónico podemos visualizarla a través de nuestras computadoras, evitándonos así tener que gastar en fotocopias como actualmente sucede.

- El principio de que la información esté siempre disponible, que existan un número infinito de copias de un texto en una biblioteca

digital sin duda alguna incrementa las oportunidades de aprendizaje, todo esto complementado.

- Se debe tener mucha precaución cuando se maneja la información en manera electrónica ya que se debe respetar los derechos intelectuales, las políticas de utilización, políticas de distribución, etc., para de esta manera no perjudicar a las personas que nos comparten su conocimiento a través de los libros.

- El sistema de Tele-inmersión es muy complejo, utiliza tecnología de último nivel, *hardware* muy costoso, algoritmos avanzados para compresión de imágenes, modelado y renderización en fin es un sistema muy completo que aún sigue en investigación y a pesar de que se han podido establecer conferencias tele-inmersivas se necesita del desarrollo de nuevas tecnologías, nuevos sistemas que permitan el óptimo funcionamiento de esta gran aplicación.

- El sistema tele-inmersivo involucra grandes cantidades de recursos tanto técnicos cómo económicos por lo que la utilización de esta aplicación en nuestro en país todavía tendrá que esperar un tiempo más, nos hace falta vencer muchas barreras sobre todo la aparte económica, que en nuestra realidad se ha convertido en la parte más importante para el desarrollo de la tecnología ya que sin recursos seremos incapaces de implementar este tipo de aplicaciones a pesar de la gran capacidad intelectual de los profesionales y estudiantes de nuestra patria.

- Los laboratorios virtuales son el complemento perfecto para el aprendizaje del estudiante, pues a pesar que un estudiante tenga la oportunidad de realizar un laboratorio real no lo puede hacer por el tiempo que se desee, ni experimentar condiciones extremas o

realizarlo en varias ocasiones, éstas posibilidades si nos lo permite un laboratorio virtual.

- Los laboratorios virtuales optimizan y ahorran recursos a las instituciones educativas, pues el equipo necesario para un laboratorio es costoso y por ende se tienen laboratorios reducidos, limitados y en riesgo pues van a ser manejados por un estudiante que debe equivocarse para aprender.

- Con un laboratorio virtual se pueden evitar accidentes, mejorar el aprendizaje, y sobre todo tener un laboratorio para cada materia o asignatura, por lo general los laboratorios son típicos de las áreas de FÍSICA y QUÍMICA y las asignaturas relacionadas con ellas, y el resto de asignaturas carecen de una parte práctica que es indispensable y que no se implementa debido a falta de presupuesto.

- La Telemedicina es una aplicación que facilita el acceso o consulta a un sistema o a un profesional de la salud desde un punto remoto, ahorrándonos tiempo y dinero además de tener el apoyo inmediato en condiciones adversas como es el caso de estar enfermo y necesitar atención o diagnóstico urgente.

- El sistema VRSV nos proporciona una alternativa para llevar a cabo reuniones entre amigos, socios, etc., a través de la red, con la ventaja de que los miembros involucrados pueden estar repartidos en varios lugares geográficos.

- El establecer reuniones con personas distantemente ubicadas es una gran ventaja para realizar todo tipo de relaciones ya sean éstas

comerciales, amistosas, culturales, etc., nos proporciona la posibilidad de conocer más gente, compartir ideas, comentarios, conocimientos con la gran características de que podemos verlas, conversar con ellas y conocerlas físicamente lo cual es muy importante cuando se trata de las relaciones personales

- Los sistemas cada día se vuelven más complejos y las aplicaciones demandan más recursos de los que le puede ofrecer un solo equipo, para ciertas aplicaciones se requieren cientos, incluso miles de equipos colaborando entre si y muchas de las veces estos equipos no se encuentran en un determinado lugar, sino distribuidos en varios sitios. A través de las redes de alta velocidad podemos utilizar las capacidades de muchos equipos distribuidos en los miembros de la red, debido a las altas velocidades que nos brindan las redes avanzadas.

- En la actualidad la educación presencial ha dejado de ser la única y mejor forma de instrucción, el campo de educación a evolucionado gracias a la tecnología pues ahora podemos tener una educación a distancia guiados por sistemas informáticos capaces de enseñar, evaluar, corregir, etc. Y la mayor parte del proceso que realizan los maestros hoy en día. Es claro que un sistema sería incapaz de brindar experiencia y conocimiento como lo hace un maestro, sin embargo es una alternativa muy interesante que ha producido óptimos resultados especialmente en personas que deseen una auto-educación.

- La tecnología *multicast* nos permite un ahorro sustancial de los recursos de la red, por lo que su utilización es prioritaria especialmente en la red tan limitada como es la de CEDIA.

- No se puede establecer una política de tiempo de espera para un usuario que desee hacer una descarga, en la cual la información posea un tamaño en *bytes* muy grande, ya que si bien es cierto las redes avanzadas se caracterizan por su gran velocidad, en nuestro país la capacidad es limitada por lo que no se puede asignar todo el ancho de banda a un solo usuario sino repartirlo entre varios, como consecuencia tendríamos que el usuario tendría que esperar horas para descargar la información requerida. En vez de esto se pueden establecer políticas de utilización que garanticen que los usuarios obtengan verdaderos beneficios.

- El ancho de banda mínimo que poseen los miembros en su última milla es insuficiente para utilizar varias aplicaciones a la vez.

- El uso de *software* de código abierto en la actualidad ha superado de sobremanera la implementación de hardware, específicamente, en lo que son equipos de enrutamiento, ya que nos ofrecen las mismas ventajas y beneficios, sumados flexibilidad a cambios futuros de funcionamiento y adaptabilidad a nuestras necesidades.

- La arquitectura de conexión provista por Telconet para la red avanzada ecuatoriana no es la adecuada, ya que, notablemente el esquema basado en túneles a través de GRE está provocando un mal desempeño de las aplicaciones que corren a través del enlace por el *overhead* que produce el establecimiento del mismo.

- El diseño de la infraestructura de red para los miembros de CEDIA está limitado a lo que provee Telconet a la red avanzada ecuatoriana, nos referimos a la incapacidad de los equipos del

núcleo al soporte de enrutamiento IPv6 y el establecimiento de conexiones *Multicast* IPv6.

- Debido a que las ventajas y beneficios que se obtienen con la marca CISCO, se ha realizado el diseño de la infraestructura de red con un equipo de esta casa fabricante, para que sea tomada en consideración por los miembros.

- Luego del análisis de la compra del equipo CISCO, se percibió que cuando los equipos se venden con el IOS *Advanced* IP *Services* incorporado son más costosos, no únicamente con la serie descrita en el diseño sino en todos los casos.

- Una de las mayores ventajas de usar el sistema operativo GNU/Linux es que puede ser instalado en computadoras con características mínimas sin afectar su rendimiento, ya que no consume altos recursos del procesador.

- Las normas de cableado estructurado para la red interna de los miembros de la red avanzada son las mismas a seguirse que para cualquier red, ya que no requieren de otros elementos de interconexión distintos a los usados comúnmente y su topología y funcionamiento son similares.

- El poseer un enlace de redundancia no necesariamente consiste en contratar un enlace dedicado de las mismas características que el usado permanentemente, por eso se aprovechó el hecho de que todos los miembros poseen acceso al Internet comercial para analizar la factibilidad de tener una conexión redundante a través de este medio.

- En la nube de Internet, todos los miembros de CEDIA tienen la misma prioridad, por lo tanto, el momento de establecer una red privada virtual deben cumplir con los mismos requerimientos para unirse entre sí y formar una red avanzada temporal hasta que se reestablezca el enlace por la red dedicada.

- El aspecto de seguridad debió ser estrictamente considerado debido a que al utilizarse una red insegura, como es el caso del Internet comercial, los usuarios no poseen la confiabilidad que al comunicarse con el enlace dedicado, por esto, nuestra solución garantiza la seguridad e integridad de la información a ser transmitida, a través, de redes privadas virtuales con protocolo IPSec.

- El uso de *software* de código abierto permitió obtener un ahorro considerable en cuanto a recursos económicos destinados a un enlace de redundancia, ya que, el principal objetivo del diseño es justamente que no signifique un aporte elevado por parte de quienes deseen tenerlo a su disposición.

- El Internet de la actualidad no soporta la ejecución de las aplicaciones de las redes avanzadas ni la implementación de los protocolos destinados al uso de estas aplicaciones, como ejemplo tenemos que el establecimiento de una comunicación *multicast* es imposible a menos que a través de túneles seamos parte de una red destinada exclusivamente al uso de esta tecnología, así tenemos el caso de la red M6Bone, a la cual necesariamente se debe pertenecer para poder utilizar *multicast*.

- La red M6Bone no tiene fines de lucro, sino el único propósito de favorecer a quienes no tienen acceso a una Red Avanzada para que puedan hacer uso de las nuevas ventajas que acarrea consigo las nuevas tecnologías en este caso *multicast* sobre IPv6.

- Con los paquetes de código abierto fácilmente se puede configurar el equipo de enrutamiento para que permita el soporte y la ejecución de las aplicaciones de las redes avanzadas, así como también el enrutamiento del tráfico que no es posible a través del Internet, además no existe ninguna restricción en el uso de *software* de código abierto, lo que no sucede con *software* licenciado, tenemos el caso por ejemplo del sistema operativo Windows, el cual obligatoriamente se exige que sea legal para su correcto desempeño.

- La aplicación más utilizada es la videoconferencia y la tecnología *multicast* beneficia enormemente la ejecución de ésta, al permitir su difusión a un grupo de participantes a través del mismo ancho de banda que el utilizado para una videoconferencia *unicast*.

5.2 RECOMENDACIONES

- Es necesario promocionar la existencia de una red avanzada en Ecuador, puesto que la mayoría de los ecuatorianos, incluyendo los estudiantes de las instituciones educativas miembros de CEDIA ignoran que tienen acceso a esta red.

- Ofertar membresías de CEDIA para incrementar el interés de las instituciones académicas en pertenecer a una red dedicada a la educación

e investigación y con ello tener a su alcance todas las ventajas y beneficios de las redes avanzadas.

- Impulsar la participación de los miembros de CEDIA en proyectos que aporten al robustecimiento de la red avanzada ecuatoriana a través de concursos, reconocimientos al mérito, entre otras actividades que despertarán mayor interés en la intervención.

- Cada miembro debe tener conocimiento de las necesidades de su red interna y con esta información diseñar planes estratégicos para el aprovechamiento máximo de la red avanzada.

- Orientar a los representantes de cada institución para que difundan la membresía a la red avanzada, por ejemplo en las universidades promover a los estudiantes a la participación en proyectos que ayuden a mejorar el rendimiento de la red, motivar a la realización de pasantías en los nodos, entre otros sin numero de actividades que pueden realizar los alumnos en mejora de la red avanzada ecuatoriana.

- Desarrollar programas educativos que tengan como objetivo principal la difusión del conocimiento del avance tecnológico a todos los usuarios, con esto se logrará una mayor acogida y se despertará el interés de nuevas instituciones de convertirse en socios estratégicos o adherentes.

- El incremento de demanda en cuanto a membresías CEDIA, se podría obtener planteando soluciones de interconexión sin limitar el acceso a un canal dedicado, dejando en claro al usuario todos los requerimientos a ser cumplidos para su correcta implementación.

- Debido a la gran desigualdad existente entre la red avanzada ecuatoriana y las demás a nivel de Latinoamérica, es necesario que todos los miembros de CEDIA colaboren con la optimización de recursos para poder ofrecer mayor cantidad de servicios sin necesidad de una nueva inversión, además sería de gran ayuda realizar convenios con el estado ecuatoriano para obtener financiamiento para la conexión internacional.

- Si se paga mensualmente por el acceso a la red avanzada, es sumamente necesario que se explote esta ventaja, ya que no es justificable que exista apenas un 3% a 5% de utilización de la red; cada representante de las instituciones miembros, está en el deber de incentivar al uso y aprovechamiento del enlace, teniendo siempre en mira la contribución al desarrollo y productividad del país.

- Las entidades educativas superiores debería poseer una biblioteca digital la misma que incluya los proyectos de titulación que sus estudiantes han realizado para que sirvan de consulta a la comunidad, sin costo alguno, con la finalidad de que esos proyectos sean guías prácticas para las distintas entidades o personas que deseen emprender proyectos similares en sus empresas, hogares, lugares de trabajo, etc., contribuyendo de esta manera a incrementar el desarrollo técnico de nuestro país. Así también debería implementar una biblioteca digital para sus estudiantes, digitalizando los libros que posee y poniéndolos a disposición de la comunidad.

- En la red de CEDIA aún no se utiliza IPv6 como protocolo nativo, se lo hace empleando túneles sobre IPv4, sin bien es cierto esta solución tiene un buen rendimiento, es utilizada como proceso de mientras se realiza la migración de IPv4 a IPv6 por lo que no es una buena solución para una red que debería utilizar IPv6 como protocolo nativo.

- La tele-inmersión es una aplicación muy exigente de recursos de ancho de banda por lo que su utilización a nivel nacional tardará algún tiempo en llegar, sin embargo debemos estar preparados pues siempre existirán proyectos de financiamiento, tal vez con ayuda gubernamental o extranjera para mejorar las características de la red y para que es en este momento el principal limitante que no permite la implementación de este tipo de aplicaciones.

- El uso de la topología tipo árbol nos permite establecer comunicaciones independientemente de fallas en puntos de red, es por esto que se recomienda su uso, así un problema existente en cualquier nodo no interrumpirá la transmisión en los restantes.

- Pese a que el ancho de banda de la ultima milla de los miembros es bajo, existen aplicaciones que pueden ser utilizadas e implementadas, como las bibliotecas digitales, laboratorios virtuales entre otros. Se recomienda que las instituciones educativas generen proyectos para implementar este tipo de aplicaciones que brindan grandes ventajas para la formación profesional de sus estudiantes.

- Para evitar la sobrecarga de procesamiento en los túneles, es necesario verificar siempre los tamaños máximo de unidad de transferencia soportados por los equipos, existen varias soluciones para evitar estos inconvenientes, así que se debe seleccionar la adecuada según los recursos que se tenga a disposición.

- Se recomienda el uso de software de código abierto debido primeramente a su costo de valor reducido o nulo, ya que acogidos a la realidad nacional, el ahorro económico es de vital importancia en nuestra sociedad especialmente en el área tecnológica, otro de los beneficios es la

flexibilidad de re-configuración según los cambios que se deseen implementar y hay que recalcar el gran numero de servicios que podemos tener a nuestra disposición incluyendo enrutamiento, calidad de servicio, seguridades, entre otros, a través de los paquetes con programación específica.

- Es sumamente necesario seguir las normas de cableado estructurado, con esto garantizamos la independencia de productos de determinadas casas fabricantes, topologías físicas o lógicas, además de la flexibilidad a cambios que se realicen a futuro que seguramente serán constantes, ya que una red avanzada, como su nombre lo indica, debe ir de la mano con el avance tecnológico.

- Las instituciones miembros de CEDIA, en especial las universidades y escuelas politécnicas deben realizar una promoción de los recursos disponibles y ofrecerlos a su comunidad, ya que el porcentaje de personas que conocen que existe una red avanzada en su institución es mínimo.

- Las instituciones miembros de CEDIA debe establecer políticas de utilización de la red avanzada, debido a que la capacidad de sus enlaces solo permiten la utilización de una sola aplicación a la vez, sin embargo esto no es razón que la red este subutilizada.

- El establecer una conexión alternativa entre los miembros de CEDIA a través de una red insegura, exige que cada nodo cumpla estrictamente con los requisitos planteados para asegurar factores como, una transmisión de calidad, soporte a las aplicaciones a ejecutarse, seguridad en la transmisión de la información.

- Aunque el planteamiento de la alternativa de conectividad, da las pautas necesarias para acceder a la red M6Bone, es recomendable que la infraestructura de red dedicada para la red avanzada sea parte de esta gran red a nivel mundial, de esta manera se tendría al alcance de todos los miembros la ventaja de pertenecer a un grupo *multicast* y así poder enviar y recibir información de este tipo.

- Es necesario que los grupos de trabajo que se reúnen en las sesiones establecidas por los miembros de CEDIA, lleven a discusión todas las ventajas que acarrean consigo el pertenecer a una red avanzada y a más de plantear proyectos, buscar cómo hacerlos realidad.

- A través de este proyecto, se dan a conocer nuevos protocolos, tecnologías, aplicaciones, servicios, que serían de gran importancia añadirlos al pénsum académico de las carreras orientadas a las redes de información: el conocimiento de esta información seguramente será de vital importancia en un futuro no muy lejano para todos los estudiantes, ya que las redes avanzadas están orientadas a ponerse a disposición del público en general.

REFERENCIAS BIBLIOGRÁFICAS

[1] CEDIA, “Consorcio Ecuatoriano para el Desarrollo del Internet Avanzado”, Agosto del 2007, http://www.cedia.org.ec/

[2] CLARA, “Cooperación Latino Americana de Redes Avanzadas”, Agosto del 2007, http://www.redclara.net/

[3] ING. CARLOS MONSALVE, Seminario Ecuador 2007:La Educación y la Investigación en la Sociedad de Información, Mayo 17, 2007, cedia_2007.ppt

[4] REUNA, “Red Universitaria Nacional”, Agosto del 2007, http://www.reuna.cl/

[5] RNP, “Rede Nacional de Ensino e Pesquisa”, Rua Lauro Muller, 31 de Octubre del 2007, http://www.rnp.br/es/backbone/index.php

[6] INSTITUTO POLITÉCNICO NACIONAL, SECRETARÍA TÉCNICA, “Metodología para el Análisis FODA”, Dirección de Planeación y Organización, Marzo 2002, http://uventas.com/ebooks/Analisis_Foda.pdf

[7] Celso Gonzales Cam, “Desarrollo de servicios digitales en las bibliotecas: nuevos retos y nuevos escenarios”, Departamento de Ciencias de la Información Pontificia Universidad Católica del Perú.

[8] Telefónica investigación y Desarrollo, Junio 2005 “Comunicaciones de Telefonía I+D “

[9] Lanier Jaron, “La Teleinmersión”, Junio 2001 http://www.investigacionyciencia.es/03005482000438/La_teleinmersi%C3%B3n.htm

[10] “Tecnologías emergentes en e-learning: Teleinmersión”, Diciembre 2005, http://www.cesga.es/content/view/395/48/lang,es/

[11] Henry Fuchs (PI), Greg Welch, “National Tele-Immersion Initiative”, Junio 2001, http://www.advanced.org/tele-immersion/Slides/I2-Mtg_files/frame.htm

[12] Magdalena Aguilar, Julián Monge-Nájera, "Evolución Tecnológica de los Laboratorios Virtuales en la universidad estatal a distancia", 1999, www.uned.ac.cr/globalNet/global/administracion/costos/articulos/AguilarMonge.pdf

[13] Ing. Marcelo Romo, "Boletín 9 INTERNET2", Junio 2003, http://www.internacional.edu.ec/academica/informatica/creatividad/uide-bits/uide-bits-09-2003.pdf

[14] Vicent M. Rodrigo Peñarrocha Miguel Ferrando Bataller, "MODELO DE REFERENCIA DE UN LABORATORIO VIRTUAL", 2001, Departamento de comunicaciones Departamento de comunicaciones Universidad Politécnica de Valencia.

[15] WIKIPEDIA, THE FREE ENCYCLOPEDIA, "Telemedicina", Noviembre 2007 http://es.wikipedia.org/wiki/Telemedicina

[16] "Curso Virtual del sistema VRVS", abril 2003, http://www.rediris.es/mmedia/vrvs/

[17] M. Sanchez, J. M. Garcia, A. F. Gómez Skarmeta, H. Martinez, "II jornadas de ingenieria telematica", Madrid (1999), "Analisis de DIS y VRML para un entorno de Simulación Distribuida aplicada a la navegación de sistemas autónomos móviles".

[18] Carlos Peces, "Desarrollo de un Modelo para un Sistema Administrador de Aprendizaje Asincrónico Basado en Objetos de Aprendizaje", 2005, Universidad de Castilla La Mancha.

[19] Juan-Mariano de Goyeneche, "COMO hacer Multicast sobre TCP/IP", Marzo 2000, http://jungla.dit.upm.es/~jmseyas/linux/mcast.como/Multicast-Como.html#toc1

[20] Ricardo Castañeda , López Arturo, "Guía Rápida de Implementación de Multicast para Internet2 en México", http://multicast.mty.itesm.mx/documentos/multicast_guia_rapida.doc

[21] Jordi Palet Martínez, "Protocolo IPv6" Enero 2004

[22] Jose Manuel Huidobro, “H.323. Multimedia sobre redes IP”, http://www.coit.es/publicac/publbit/bit109/quees.htm

[23] Jyh-Ming Lien, Ruzena Bajcsy, “Model Driven Compression of 3-D Tele-Immersion Data”, Diciembre 2006, www.eecs.berkeley.edu/Pubs/TechRpts/2006/EECS-2006-170.pdf

[24] MICROSOFT, “Implementación de una solución empresarial de comunicaciones activas en Microsoft”, Agosto 2004, http://www.microsoft.com/spain/technet/recursos/articulos/19110302.aspx#Ventajas

[25] Marcela Rincón y Alejandra Rodríguez, “Programa de Ingeniería Biomédica”, “Escuela de Ingeniería de Antioquia -Instituto de Ciencias de la Salud”, http://itzamna.uam.mx/alfonso/index.html.

[26] Espin Albán, Javier Gerardo, “Diseño de una infraestructura multicast usando IPV6 sobre dominios IPV4 para brindar aplicaciones básicas de telemedicina”, 2004

[27] Network Working Group M., “Limitations of Internet Protocol Suite for Distributed Simulation the Large Multicast Environment”, 1999, PullenRFC 2502.

[28] WIKIPEDIA, THE FREE ENCYCLOPEDIA, ”HTTP”, Wikipedia.org, Noviembre del 2007 http://es.wikipedia.org/wiki/HTTP

[29] WIKIPEDIA, THE FREE ENCYCLOPEDIA, ”FTP”, Wikipedia.org, Noviembre del 2007 http://es.wikipedia.org/wiki/FTP

[30] WIKIPEDIA, THE FREE ENCYCLOPEDIA, ”SCP”, Wikipedia.org, Noviembre del 2007 http://es.wikipedia.org/wiki/SCP

[31] WIKIPEDIA, THE FREE ENCYCLOPEDIA, ”DNS”, Wikipedia.org, Noviembre del 2007 http://es.wikipedia.org/wiki/DNS

[32] WIKIPEDIA, THE FREE ENCYCLOPEDIA, ”TCP”, Wikipedia.org, Noviembre del 2007 http://es.wikipedia.org/wiki/TCP

[33] WIKIPEDIA, THE FREE ENCYCLOPEDIA, ”UDP”, Wikipedia.org, Noviembre del 2007 http://es.wikipedia.org/wiki/UDP

[34] KIOSKEA.NET, “Internet Protocolos RTP/RTCP”, Knowledge Kiosk, Marzo 2008 http://es.kioskea.net/internet/rtcp.php3

[35] WIKIPEDIA, THE FREE ENCYCLOPEDIA, ”SMTP”, Wikipedia.org, Noviembre del 2007 http://es.wikipedia.org/wiki/SMTP

[36] WIKIPEDIA, THE FREE ENCYCLOPEDIA, ”RSVP”, Wikipedia.org, Noviembre del 2007 http://es.wikipedia.org/wiki/RSVP

[37] Agustín Santos-Méndez, Luis Rodero-Merino, Andrés Leonardo Martínez-Ortíz, Daniel Izquierdo-Cortázar, “Framework basado en AOP para la simulación distribuida según el estándar IEEE-1516”, Laboratorio de Algoritmia Distribuida y Redes Escuela Superior de Ciencias Experimentales y Tecnología Campus de Móstoles (Madrid), Febrero 2006, http://gsyc.es/~lrodero/papers/propuesta_hla.pdf

[38] Protocolos de Voip H323, Noviembre 2007 http://www.voipforo.com/H323/H323objetivo.php

[39] CISCO 2801 Bundle WIC-1SHDSL-V3 SP Svcs 64F/192D (B), http://www.computerpool.de/artikel/router_180/c2801-shdsl-v3-k9-cisco-2801-dsl-bundle_29451062/

[40] Redes Virtuales VLANs, http://www.textoscientificos.com/redes/redes-virtuales.

[41] Ebay.es, http://www.rabit.ru/images/trade_fprv_17411.jpg

[42] WIKIPEDIA, THE FREE ENCYCLOPEDIA, “Ethernet”, Wikipedia.org, Noviembre del 2007, http://es.wikipedia.org/wiki/Ethernet

[43] Sandra Milena Sandoval Carrillo, “ANÁLISIS DEL PROTOCOLO IPSec EN AMBIENTE IPv6”, PAMPLONA, COLOMBIA NOVIEMBRE http://kmconocimiento.unipamplona.edu.co/KMportal/hermesoft/portalIG/home_1/recursos/tesis/contenidos/pdf_tesis/pdf_2/02052007/analisis_del_protocolo_ipsec.pdf2006

[44] Carlos Ralli Ucendo, “Mecanismo de Transición IPv4 - IPv6” 2006, www.cu.ipv6tf.org/pdf/carlos_ralli_transitiontutorial.pdf

[45] Winston Jesus Ortega “Coexistencia entre IPv4 e IPv6”, Noviembre 2007, http://neutron.ing.ucv.ve/revista-e/No5/WOrtega.htm.

[46] “Fiche descriptive du M6Bone”, Noviembre 2007, http://www.renater.fr/spip.php?article91

[47] “NT MBone Walkthrough”, Noviembre 2007 http://netlab.gmu.edu/nt-mbone/

[48] “How to contact us via MBone Tools”, http://www.ciel.pl/mbone.html

[49] WIKIPEDIA, THE FREE ENCYCLOPEDIA, “Fast_Ethernet”, Wikipedia.org, Noviembre del 2007, http://es.wikipedia.org/wiki/Fast_Ethernet

[50] WIKIPEDIA, THE FREE ENCYCLOPEDIA, “Gigabit_Ethernet”, Wikipedia.org, Noviembre del 2007, http://es.wikipedia.org/wiki/Gigabit_Ethernet

[51] WIKIPEDIA, THE FREE ENCYCLOPEDIA, “IPSec”, Wikipedia.org, Noviembre del 2007, http://es.wikipedia.org/wiki/IPsec

[52] WIKIPEDIA, THE FREE ENCYCLOPEDIA, “IEEE_802.1Q”, Wikipedia.org, Noviembre del 2007, http://es.wikipedia.org/wiki/IEEE_802.1Q

[53] WIKIPEDIA, THE FREE ENCYCLOPEDIA, “MGCP”, Wikipedia.org, Noviembre del 2007, http://es.wikipedia.org/wiki/MGCP

[54] WIKIPEDIA, THE FREE ENCYCLOPEDIA, “H.323”, Wikipedia.org, Noviembre del 2007, http://es.wikipedia.org/wiki/H.323

[55] WIKIPEDIA, THE FREE ENCYCLOPEDIA, “G.711”, Wikipedia.org, Noviembre del 2007, http://es.wikipedia.org/wiki/G.711

[56] VOIPFORO,“Codecs”,VoIPForo, Noviembre del 2007, http://www.voipforo.com/codec/codecs.php

[57] WIKIPEDIA, THE FREE ENCYCLOPEDIA, “G.729.a”, Wikipedia.org, Noviembre del 2007, http://en.wikipedia.org/wiki/G.729a

[58] ASOCIACIÓN DE INGENIEROS INFORMÁTICOS DE EXTREMADURA,"Open SimMPLS", AIIEx, Noviembre del 2007, http://gitaca.unex.es/opensimmpls/web/es/indiceES.html

[59] WIKIPEDIA, THE FREE ENCYCLOPEDIA, "DES", Wikipedia.org, Noviembre del 2007, http://es.wikipedia.org/wiki/Data_Encryption_Standard

[60] WIKIPEDIA, THE FREE ENCYCLOPEDIA, "AES", Wikipedia.org, Noviembre del 2007, http://es.wikipedia.org/wiki/AES

[61] WIKIPEDIA, THE FREE ENCYCLOPEDIA, "Topologia tipo arbol", Wikipedia.org, Noviembre del 2007, http://es.wikipedia.org/wiki/Red_en_Arbol

[62] WIKIPEDIA, THE FREE ENCYCLOPEDIA, "High level Architecture", Wikipedia.org, Noviembre del 2007,

[63] http://en.wikipedia.org/wiki/High_Level_Architecture

[64] ALFONSO ARAUJO CÁRDENAS,"Redes y sus Topologías", Geocities, Noviembre del 2007, http://mx.geocities.com/alfonsoaraujocardenas/topologias.html

[65] Br. ANDREINA CARRERO, "Normas ANSI ISO IEEE para cableado UTP", Monografias.com, Noviembre del 2007, http://www.monografias.com/trabajos11/utp/utp.shtml

[66] FRANCISCO BOLAÑOS, "Propuesta de Migración Red CUDI", Primavera 2006 CUDI, Noviembre del 2007, http://www.cudi.edu.mx/primavera_2006/presentaciones/redes_francisco_bolanos.pdf

[67] CIAO, "CISCO 2801 DSL Bundle", Noviembre del 2007, Ciao Shopping Intelligence, http://www.ciao.es/Cisco_2801_DSL_Bundle__625655

[68] JOSE LUIS ARCEIZ BAQUERO, "Multicast Mbone", Curso de Doctorado Telemática, Diciembre del 2007, http://usuarios.lycos.es/arceizb/MULTICAST%20MBONE.pdf

[69] JOYCE K. REYNOLDS, SANDY GINOZA, “RFC 3956 on Embedding the Rendezvous Point Adress in an Ipv6 Multicast Adress ”, USC/Information Sciencies Institute, Diciembre del 2007, http://www1.ietf.org/mail-archive/web/ietf-announce/current/msg00693.html

[70] RENATER, “Ipv6 Multicast”, Le Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche, Diciembre del 2007, http://www.renater.fr/spip.php?article459

[71] RENATER, “Listes de diffusion”, Le Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche, Diciembre del 2007, https://listes.renater.fr/sympa/info/m6bone

[72] GUILLERMO DAPORTA, “Glosario”, Diciembre del 2007, http://www.gratisweb.com/gulle79/glosario/r.htm

[73] ARIEL TARANTO, “cbq”, Diciembre del 2007, http://beta.redes-linux.com/manuales/ancho_banda/redhat-bwidth-shaper.txt

[74] RETRONET, “Control de ancho de banda con CBQ-INIT”, Diciembre del 2007, http://beta.redes-linux.com/manuales/ancho_banda/control_ancho_banda_cbqinit.pdf

[75] Presentación Power Point, CUDI, Corporación Universitaria para el Desarrollo de Internet, Alternativas de acceso a la red de Internet 2

[76] UNIDAD DE NEGOCIO DE DATOS: Alternativas de acceso a la red de Internet 2”, Coorporación Universitaria para el Desarrollo de Internet, Diciembre del 20007, CUDI_2005V2_4.ppt

[77] CISCO SYSTEMS, “Multicast over a GRE Tunnel”, Diciembre del 2007, http://www.cisco.com/en/US/tech/tk828/technologies_configuration_example09186a00801a5aa2.shtml

[78] OPERATION OF A NODE IN THE EXPERIMENTAL IPV6 MULTICAST NETWORK, “M6BONE”, Christian Lazo R.1 Roland Glöckler2, Recibido el 16 de marzo de 2005, aceptado el 6 de julio de 2005

[79] MAX LÓPEZ, RICARDO CASTAÑEDA, ARTURO SERVÍN, “Arquitectura de IP Multicast para backbone de Internet 2 en México”, Diciembre del 2007, http://usuario.cicese.mx/~mparra/propmc.html

[80] WIKIPEDIA, THE FREE ENCYCLOPEDIA, “VPN”, Wikipedia.org, Diciembre del 2007, http://euitio178.ccu.uniovi.es/wiki/index.php/VPN

[81] MARCO DAVIDS, “Linux Advanced Routing & Traffic Control HOWTO”, Linux.com, http://www.linux.com/base/ldp/howto/Adv-Routing-HOWTO/lartc.ipv6-tunnel.html

[82] CISCO SYSTEMS, “Why can not browse the Internet when using a GRE Tunnel”, Diciembre del 2007, http://www.cisco.com/warp/public/105/56.pdf

[83] ANDREU VEÁ BARÓ, “Evolución de la Tecnología de Acceso a Internet”. Universidad de La Salle de Bogotá, Mayo 2002, http://www.tdx.cat/TESIS_URL/AVAILABLE/TDX-1104104-101718//Tavb08de23.pdf

[84] DEPARTAMENTO DE SEÑALES, “Upgrading red”, Universidad Politécnica de Madrid, Marzo 2006, http://209.85.165.104/search?q=cache:kNwB5skgw4kJ:www.pmde.gob.pe/archivos/Informes/EF-GE/TITULO%2520III_CAPITULO%25203.4_DESCRIP_TECN_ALT_SELECCIONADA.pdf+factor+de+simultaneidad+10%25+isp&hl=es&ct=clnk&cd=25&gl=ec

[85] WIKIPEDIA, THE FREE ENCYCLOPEDIA, “MCU”, Wikipedia.org, Marzo 2008, http://es.wikipedia.org/wiki/MCU

[86] HUMBERTO SANLÉZ, ”Cabecera de una dirección IPv4”, Marzo 2008, http://humbertofp.wordpress.com/2008/01/23/cabecera-de-una-direccion-ipv4/

Glosario de Términos

2D	Dos dimensiones
3D	Tres dimensiones
3DES	Algoritmo de triple cifrado DES.
6to4	Túneles que encapsulan IPv6 en IPv4
AAL1	ATM *Adaptation Layer* 1 ó Capa 1 de adaptación ATM
AB	Ancho de banda
AccesGrid	Red de cómputo en malla
ACR/NEMA	Estándar para manejo y transmisión de imágenes digitales
ACR/NEMA DICOM 3.0	Estándar para manejo y transmisión de imágenes digitales
ADSL	*Asymetric Digital Suscriber Line* ó Línea digital asimétrica de suscriptor

AES	*Advanced Encyption Standard* ó Estándar de encripción avanzado
AH	*Authentication Header* ó Cabecera de autenticación
ALICE	América Latina Interconectada con Europa
Ampath	*Americas Path Network* ó Red de las américas
Ancho de banda	Rango de frecuencias en el que se concentra la mayor parte de la potencia de la señal.
ANSI/TIA/EIA-568-B	Norma para construcción comercial de cableado de telecomunicaciones
ANSI/EIA/TIA-569-A	Norma de construcción comercial para vías y espacios de telecomunicaciones
ANSI/TIA/EIA-606-A	Norma de administración para la infraestructura de telecomunicaciones en edificios comerciales
ANSI/TIA/EIA-607-A	Requisitos de puesta a tierra y protección para telecomunicaciones en edificios comerciales
ANSI	Instituto Nacional Americano de Normas

Anycast	Difusión a cualquier interfaz de un equipo que tiene la dirección especificada.
Apple talk	Protocolo de enrutamiento
Asintel	Distribuidor de Equipos de *Networking*
ASM	*Any Source Multicast* ó Multidifusión de cualquier origen
ATM	*Asynchronous Transfer Mode* ó Modo de transferencia asincrónico
Autenticación	Acción de verificación de identidad.
Backbone	Principales conexiones troncales de una red.
BGP	*Border Gateway Protocol* ó Protocolo de puerta de enlace de borde
Bit	Unidad de información cuyo valor puede ser 1 Lógico o 0 Lógico
BOOTP	Protocolo de arranque
Broadcast	Difusión total ó transmisión de información desde un emisor a todos los receptores posibles

Byte	Unidad de datos compuesta por 8 bits
CAITECH	Instituto de Tecnología de California
CAPE-OPEN	*Computer Aided Process Engineering Open Simulation Enviroment* ó Ambiente de simulación abierta de procesamiento de ingeniería asistido por computadora
CBQ	*Class-Based Queuing* ó Encolada basado en clases
CBT	*Core-Based Trees* ó Árboles basados en núcleo
CEO	Centro de Ingeniería y Operaciones
CISCO	Fabricante de equipos de *networking*
Cisco pix	Linea de *firewalls* de cisco
CEDIA	Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado
CEREP	Cuenta de Reactivación Productiva y Social, Desarrollo Científico -Tecnológico y Estabilidad Fiscal

Chat	Sistema de conversación escrita
Checkpoint NG	*Firewall* en *hardware*
Checksum	Mecanismo de verificación de errores
CHS	Distribuidor de computadores y equipos de *networking*
CLARA	Consorcio Latino Americano de Redes avanzadas
Cluster	Agrupación para trabajo conjunto
CMS	*Content Management System* ó Sistema de administración de contenido
Codec	Codificador-Decodificador
Core	Núcleo o centro
CoS	*Class of service* ó Clase de servicio
CPU	*Central processing unit* ó Unidad central de procesamiento

CSI	*Customer Service Inquiri* ó Petición de servicios de cliente
Datagrama	Paquete de información
DARPA	*Defense Advanced Research Projects Agency* ó Agencia de investigación de proyectos avanzados de defensa
Data Compression Ratio	Tasa de compresión de datos
Data rate	Tasa de transferencia de datos
DDR SDRAM	Nueva generación de memorias RAM para computadores
DES	*Data encryption Standard* ó estándar de encripción de datos
DHCP	*Dynamic Host Configuration Protocol* ó Protocolo de configuración dinámica de *hosts*
DIS	*Distributed Interactive Simulation* ó Simulación interactiva distribuida
DLINK	Fabricante-distribuidor de equipos de *networking*

DMZ	Zona desmilitarizada, ó de menor seguridad
DNS	*Domain Name System* ó Sistema de nombres de dominio
DOI	*Domain of Interpretation* ó Dominio de interpretación
DoS	*Denial of Service* ó Denegación de servicio
DragonFlyBSD	Sistema operativo basado en los sistemas BSD
DSL	*Digital Suscriber Line* ó Línea digital de suscriptor
Dual router	*Router* que puede manejar IPv4 e IPv6
DVMRP	*Distante Vector Multicast Routing Protocol* ó Protocolo de enrutamiento multidifusión vector distancia
E-books	Libros digitales
E-learning	Aprendizaje por Internet
E-mail	Correo electrónico

EIA	Alianza de Industrias Electrónicas
Encaminador	Enrutador
Encriptación	Cifrado de los datos
Enrutador	Dispositivo para interconexión de redes de computadores, que opera en la capa tres del modelo ISO/OSI
ESP	*Encapsulating Security Payload* ó Payload asegurado con encapsulación
Ethernet	Estándar de comunicación para redes de área local, semejante a IEEE 802.3 10Base5
Federate	Miembro ó federado
Federation	Conjunto de federados
Firewall	Dispositivo ó *software* que permite implementar seguridades de red.
Flash	Memoria volátil
Flood	Inundación

FODA	Análisis de Fortalezas – Oportunidades – Debilidades – Amenazas
Fragmentación	Segmentado de los paquetes o tramas de datos
Framing PPP	Entramado del protocolo punto a punto
FreeBSD	Sistema operativo gratuito derivado de los sistemas BSD
FreeS/Wan	*Red Wan* gratuita para Linux
FTP	*File transfer protocol* ó Protocolo de transferencia de archivos
G.711	Estándar de compresión de audio que proporciona un flujo de datos de 64 kbps.
G.722	Estándar de compresión de audio, que proporciona un flujo de datos de 64 kbps, 48 kbps o 32 kbps
G.723	Estándar de compresión de audio que proporciona un flujo de datos de 5.3 kbps o 6.4 kbps
G.728	Estándar de compresión de audio que proporciona un flujo de datos de 16 kbps

GB	*Gigabytes*
Gbps	*Gigabits* por segundo
GÉANT2	Red Avanzada europea
GIF	*Graphics Interchange Format* ó Formato de intercambio de gráficos
Global Crossing	Proveedor de servicios de internet antes conocido como IMPSAT Ecuador
GNU	*GNU is not unix* ó GNU no es Unix
GPIB	*General Purpose Interface* Bus ó Bus de interfaz de propósito general
GRE	*Generic Routing Encapsulation* ó Encapsulación de enrutado genérico
GREUNA	Nueva versión de REUNA2 con 1GB de capacidad
GSM	*Global System for Mobile communications* ó Sistema global para comunicaciones móviles

H.225	Protocolo de control de llamada que permite establecer una conexión y una desconexión
H.245	Protocolo de control usado en el establecimiento y control de una llamada
H.261	Estándar de compresión de video, diseñado para una tasa de datos múltiplo de 64 Kbps
H.263	Estándar de compresión de video, diseñado para bajas velocidades, pero en la actualidad ha sido mejorado para reemplazar a H.261
H.310	Estándar para videoconferencia sobre ATM, a velocidades que van desde 8 Mbps a 16 Mbps.
H.320	Estándar para videoconferencia sobre RDSI
H.321	Estándar para videoconferencia sobre ATM
H.323	Estándar para videoconferencia utilizando protocolos TCP/IP.
Hardware	Se usa para describir a los elementos físicos de un equipo de funcionalidad eléctrica o electrónica

Header	Se usa para referirse a las cabeceras de los empaquetados de datos
HeadTracking	*Hardware* para buscar localizaciones
HIS	Sistemas de Información Hospitalaria
HLA	*High Level Architecture* ó Arquitectura de alto nivel
Host	Se usa para referirse a un dispositivo de red
HTML	*HyperText Markup Language* ó Lenguaje de marcas de hipertexto
HTTP	*HyperText Transfer Protocol* ó Protocolo de transferencia de hipertexto
IEEE 802 MAC	Protocolo de sub capa MAC para 802.3.
IDS	*Intrusion Detection System* ó Sistema de detección de intrusiones
IGMP	*Internet Group Management Protocol* ó Protocolo de administración del grupo Internet

IGMPv2	*Internet Group Management Protocol version* 2 ó Protocolo de administración del grupo Internet versión 2
IKE	*Internet Key Exchange* ó Intercambio de llaves por Internet
IITAP	*International Institute of Theoretical and Applied Physics* ó Instituto internacional de física teórica y aplicada
INTERNET2	Red Avanzada de Estados Unidos
Internet Explorer	Navegador de internet propietario de Microsoft provisto con las distribuciones de Windows
INTRANET	Conjunto de equipos y servicio pertenecientes a una misma organización
IOS	*Inter Operating System* ó Sistema interoperativo
IPng	IP nueva generación o IPv6
IPSec	*Internet Protocol Security* ó Seguridad de Protocolo Internet
IPv4	*Internet Protocol version* 4 ó Protocolo de Internet versión 4

IPv6	*Internet Protocol version* 6 ó Protocolo de Internet versión 6
IPX	Protocolo de enrutamiento
IRC	*Chat*
ISABEL	Sistema de video conferencia usado en las redes avanzadas
ISO	*International Standards Organization* ú Organización de estándares internacionales
ITU-T	Unión internacional de telecomunicaciones – área de telecomunicaciones
IVI	*Interchangeable Virtual Instruments* ó Instrumentos virtuales intercambiables
JBIG	*Joint Bilevel Image Group* ó Grupo de imagines de dos niveles conjuntos
Jitter	Variaciones en el retardo de tiempo

JPEG	*Joint Photographic Coding Experts Group* ó Grupo de expertos en codificación fotográfica conjunta
Kbps	Kilobits por segundo
KLIPS	*kernel IPsec*
L2F	*Layer 2 Forwarding* ó Paso de información de capa 2
L2TP	*Layer 2 Tunneling Protocol* ó Protocolo de entunelamiento de capa 2
Laboratorio virtual	Conjunto de equipos dispuestos en un lugar lejano al usuario para que este los use remotamente
LACNIC	Entidad encargada de la asignación de nombres para Latinoamérica
LAN	*Local Area Network* ó Red de área local
LCMS	*Learning Content Management System* ó Sistema de administración de contenido de aprendizaje

Learningware	Sistema de gestión de desarrollo y distribución de material educativo sobre redes públicas y privadas
Linux	Sistema operativo gratuito
LMS	*Learning Managment System* ó Sistema de administración de aprendizaje
Linksys	Fabricante de equipos de *networking*
M-JPEG	*Motion* JPEG ó JPEG en movimiento
M6bone	Mbone para IPv6
MacOS X	Sistema operativo basado en los sistemas BSD y que se usan en computadores Macintosh
Mandrake	Distribución de Linux
MB	Megabytes
Mbone	*Multicast Bone* ó Red dedicada para multidifusión sobre IPv4
Mbps	*Megabits* por segundo

MD2	*Message Digest* 2, algoritmo de encripción
MD5	*Message Digest* 5, algoritmo de reducción criptográfico de 128 bits.
MFEA	*Multicast Forwarding Engine Abstraction* ó Abstracción de máquina de paso de multidifusión
MLD	*Multicast Listener Discovery* ó Descubrimiento de escuchas multidifusión
MOSPF	*Multicast Open Short Path First* ó Primero el camino abierto más corto en multidifusión
Mozzila Firefox	Navegador de internet gratuito
MP-3	Estándar de compresión de audio
MP-BGP	*Multiprotocol* BGP ó BGP multiprotocolo
MPEG	*Motion Picture Experts Group* ó Grupo de expertos en el movimiento de imágenes
MPLS	*Multi Protocol Label Switching*
Mrouter	*Multicast router* ó enrutador multidifusión

MRP	*Multicast Routing Protocols* ó Protocolos de enrutamiento multidifusión
MSS	*Maximun Segment Size* ó Tamaño máximo de segmento
MTU	*Maximum Transfer Unit* ó Unidad máxima de transferencia
Multicast	Multidifusión ó transmisión de información desde un emisor a varios receptores
NAPT	*Network Address Port Translator* ó Traductor de puertos y direcciones de red
NAT	*Network Address Translation* ó Traducción de direcciones de red
NAT-PT	*Network Address Translation - Protocol Translation* ó Traducción de direcciones de red – Traducción de protocolos, mecanismo de traducción de formatos de paquete IPv4 a IPv6 y viceversa
NEG	*Network Engineering Group* ó Grupo de ingeniería de red
NetBSD	Sistema operativo basado en los sistemas BSD

Netscape Communicator	Navegador de Internet Gratuito
Netscreen	Fabricante de equipos de *networking*
Network commerce	Comercio por red
Networking	Se usa para referirse al trabajo en red o para la interconexión entre redes
NOC	*Network Operation Center* ó Centro de operaciones de red
Nokia	Fabricante de equipos de *networking*
Nortel	Fabricante de equipos de *networking*
NTE	*Network Test Editor* ó Editor de pruebas de red
NTP	*Network Time Protocol* ó Protocolo de tiempo de red
Open source	Se refiere al software gratuito
OpenBSD	Sistema operativo basado en los sistemas BSD

OpenSSH	*Open Secure Shell* ó Shell seguro abierto
OpenVPN	*Open Virtual Private Network* ó Red privada virtual abierta
Oracle	Motor de bases de datos propietario
OSI	*Open systems interconnected* ó Interconexión de sistemas abiertos
OSPF	*Open Short Path First* ó Camino abierto más corto primero
Overhead	Sobrecarga de mensajes informativos, y sin información de datos
P2P	*Point to point* ó Punto a punto
PACS	*Picture Archiving and Communications Systems* ó Archivado de imagines y sistemas de comunicaciones
Payload	Datos de capa superior en un empaquetado de información
PDA	Dispositivo computacional portátil, más pequeño que una *laptop*

PDF	*Portable document format* ó Formato de documento portátil, definido como estándar como ISO 32000
PIM	*Protocol Independent Multicast* ó Multidifusión independiente del protocolo
PIM-DM	*Protocol Independent Multicast Dense Mode* ó Multidifusión independiente del protocolo modo denso
PIM-SM	*Protocol Independent Multicast Sparse Mode* ó Multidifusión independiente del protocolo modo esparcido
Píxel	Es la menor unidad homogénea en color que forma parte de una imagen digital.
Plug&Play	Conectar y usar
Pluto	Demonio del protocolo IKE
PoPs	*Points of Presence* ó Puntos de presencia
Proxy	Servidor que permite el almacenamiento y reuso de los elementos requeridos por los usuarios de los servicios web

Prune	Mensaje de supresión
PXI	PCI *eXtensions for Instrumentation* ó Extensiones PCI para instrumentación
Q.931	*Digital Subscriber Signalling* ó Señalización de suscriptor digital
QoS	*Quality of Service* ó Calidad de servicio
Quagga	*Software* de enrutamiento *open source*
RAM	*Random access memory* ó memoria de acceso aleatorio
RAS	*Registration, Admission and Status* ó Registro, admisión y estado
RAT	*Robust Audio Tool* ó Herramienta de audio robusto
RCTS	*Rede Ciência, Tecnologia e Sociedade* ó Red de ciencia tecnología y sociedad
RDSI	Red Digital de Servicios Integrados

Red Hat	Distribución de Linux
Renater	*Le Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche* ó Red nacional de telecomunicaciones para la tecnología, la enseñanza y la investigación
REUNA	Red universitaria nacional
REUNA2	Red universitaria nacional versión 2
REUNA Tec	Gerencia técnica de REUNA
RIP	*Routing Information Protocol* ó Protocolo de información de enrutamiento
RIS	Sistema de información radiológica
RNP	Red nacional de enseñanza e investigación
Router	Enrutador
RP	*Rendezvous Point* ó Punto de encuentro
RPM	Paquete de instalación en Linux

RS-232	*Recommended Standard* 232 ó Estándar-Recomendación 232
RSVP	*ReSource reserVation Protocol* ó Protocolo de reservación de recursos
RTI	*RunTime Infraestructure* ó Infraestructura de ejecución
RTCP	*Real-Time Transport Control Protocol* ó Protocolo de control de transporte en tiempo real
RTP	*Realtime Transport Protocol* ó Protocolo de transporte en tiempo real
SCORM	*Sharable Content Object Reference Model* ó Modelo de referencia de contenido de objetos que se pueden compartir
SCP	*Secure copy protocol* ó protocolo de copia segura
SCPI	*Standard Commands for Programmable Instruments* ó Comandos estándar para instrumentos programables
SDH	*Synchronous Digital Hierarchy* ó Jerarquía digital sincrónica

SDR	*Sesion Directory* ó Directorio de sesión
Security Policy	Política de seguridad
SERVITEL	Proveedor de servicios de puesta a punto de cableado estructurado
SGML	*Standard Generalized Markup Language* ó Lenguaje de marcas estándar generalizado
SHA	*Secure Hash Algoritm* ó Algoritmo de *hash* seguro
SIIT	Algoritmo de transición *stateless*
SIMNET	*Simulator Networking* ó simulador de *networking*
Skype	Red de telefonía IP que funciona en el Internet comercial
SMTP	*Simple Mail Transfer Protocol* ó Protocolo simple de transferencia de correo
SNMP	*Simple Network Management Protocol* ó Protocolo simple de administración de red

SOCKSv5	Mecanismo de traducción de formatos de paquete IPv4 a IPv6 y viceversa
Software	Se usa para describir a los elementos lógicos que le otorgan la funcionalidad a un equipo computacional
SPD	*Security Policy Database* ó Base de datos de políticas de seguridad
SPI	*Security parameter index* ó índice de parámetros de seguridad
SPT	*Short Path First* ó Primero el camino más corto
SQL	*Structured Query Language* ó Lenguaje de consultas estructuradas
SSH	*Secure Shell*
SSL	*Secure Sockets Layer* ó Capa de sockets seguros
SSO	Servicio de Soporte a Operaciones
Stack	Estructura de datos.

Sun Solaris	Sistema operativo no gratuito, predecesor de Linux
SUSE	Distribución de Linux
Symantec	Fabricante de equipos y *software* de *networking*
T.120	Estándar de compresión de datos
Talking books	Libros hablados para personas no videntes
TCP/IP	*Trasmission control protocol /Internet protocol*
Tcpdump	Herramienta de Linux para capturar paquetes
TIA	Asociación de Industrias de Telecomunicaciones
TLS	*Transport Layer Security* ó Seguridad de capa de transporte
Transelectric	Proveedor de salida internacional a Internet en el Ecuador
Telconet	Proveedor de Servicios de Internet en el Ecuador
Telemedicina	Aplicación de las redes avanzadas que permite realizar prácticas médicas a distancia

Tele-inmersión	Aplicación de las redes avanzadas que permite simular la presencia de los conferencistas
Teléfono IP	Dispositivo de comunicación audible, que transmite información usando el protocolo IP
Telnet	Protocolo de terminal remota
TICs	Tecnologías de la Información y comunicación
TotalTek	Distribuidor de equipos de *networking*
UDP	*User datagram protocol* ó Protocolo de datagramas de usuario
Unicast	Envío de información de un emisor a un solo receptor
URI	*Uniform Resource Identifier* ó Identificador de recurso uniforme
URL	*Uniform Resource Location* ó Ubicación de recurso uniforme
URN	*Uniform Resource Name* ó Nombre de recurso uniforme

US Robotics	Fabricante de equipos de *networking*
VBR	*Variable Bit Rate* ó tasa de bits variable
VIC	*Video Conference* ó Video conferencia
VISA	*Virtual Instrument Software Architecture* ó Arquitectura de software de instrumentos virtuales
VLANs	*Virtual Local Area Network* ó Red de área local virtual
VoFR	*Voice over Frame Relay* ó Voz sobre *Frame Relay*
VoIP	*Voice over IP* ó Voz sobre IP
VPN	*Virtual Private Network* ó Red privada virtual
VRVS	*Virtual Room Videoconferencing System* ó Sistema de video-conferencia de habitación virtual
VXI	VME *eXtensions for Instrumentation* ó Extensiones VME para instrumentación

Vyatta	*Software open source* para enrutamiento
WAN	*Wide Area Network* ó Red de área amplia
WBD	*White Board* ó Pizarra compartida usando *multicast*
Web	Se usa para referirse a la red Internet o a un servicio http
WID	*Wireless Information Devices* ó Dispositivos de información inalámbrica
Windows	Grupo de sistemas operativos propietarios de *Microsoft*
XML	*eXtensible Markup Language* ó lenguaje de marcas extensible
Xorp	*eXtensible Open Router Platform ó* Plataforma de enrutamiento abierta y extensible

Anexo 1:

Características *router* cisco serie 2800

ANEXO 1: CARACTERÍSTICAS ROUTER CISCO SERIE 2800

Cisco 2800 Series Integrated Services Routers

Cisco Systems®, Inc. is redefining best-in-class enterprise and small- to- midsize business routing with a new line of integrated services routers that are optimized for the secure, wire-speed delivery of concurrent data, voice, video, and wireless services. Founded on 20 years of leadership and innovation, the Cisco® 2800 Series of integrated services routers (refer to Figure 1) intelligently embed data, security, voice, and wireless services into a single, resilient system for fast, scalable delivery of mission-critical business applications. The unique integrated systems architecture of the Cisco 2800 Series delivers maximum business agility and investment protection.

Figure 1. Cisco 2800 Series

Product Overview

The Cisco 2800 Series comprises four platforms (refer to Figure 1): the Cisco 2801, the Cisco 2811, the Cisco 2821, and the Cisco 2851. The Cisco 2800 Series provides significant additional value compared to prior generations of Cisco routers at similar price points by offering up to a fivefold performance improvement, up to a tenfold increase in security and voice performance, embedded service options, and dramatically increased slot performance and density while maintaining support for most of the more than 90 existing modules that are available today for the Cisco 1700, Cisco 2600, and Cisco 3700 Series.

The Cisco 2800 Series features the ability to deliver multiple high-quality simultaneous services at wire speed up to multiple T1/E1/xDSL connections. The routers offer embedded encryption acceleration and on the motherboard voice digital-signal-processor (DSP) slots; intrusion prevention system (IPS) and firewall functions; optional integrated call processing and voice mail support; high-density interfaces for a wide range of wired and wireless connectivity requirements; and sufficient performance and slot density for future network expansion requirements and advanced applications.

Secure Network Connectivity for Data, Voice, and Video

Security has become a fundamental building block of any network. Routers play an important role in any network defense strategy because security needs to be embedded throughout the network. The Cisco 2800 Series features advanced, integrated, end-to-end security for the delivery of converged services and applications. With the Cisco IOS® Software Advanced Security feature set, the Cisco 2800 provides a robust array of common security features such as a Cisco IOS Software Firewall, intrusion prevention, IPSec VPN, Secure Socket Layer (SSL) VPN, advanced application inspection and control, Secure Shell (SSH) Protocol Version 2.0, and Simple Network Management Protocol (SNMPv3) in one secure solution set. Additionally, by integrating security functions directly into the router itself, Cisco can provide unique intelligent security solutions other security devices cannot, such as network admissions control (NAC) for antivirus defense; Voice and Video Enabled VPN (V3PN) for quality-of-service (QoS) enforcement when combining voice, video, and VPN; and Dynamic Multipoint VPN (DMVPN), Group Encrypted Transport (GET) VPN, and Easy VPN for enabling more scalable and manageable VPN networks. In addition, Cisco offers a range of security acceleration hardware such as the intrusion-prevention network modules and advanced integration modules (AIM) for encryption, making the Cisco 2800 Series the industry's most robust and adaptable security solution available for branch offices. As Figure 2 demonstrates, using a Cisco 2800 Series uniquely enables customers to deliver concurrent, mission-critical data, voice, and video applications with integrated, end-to-end security at wire-speed performance.

Converged IP Communications

As shown in Figure 2, the Cisco 2800 Series can meet the IP Communications needs of small-to-medium sized business and enterprise branch offices while concurrently delivering an industry-leading level of security within a single routing platform. Cisco CallManager Express (CME) is an optional solution embedded in Cisco IOS Software that provides call processing for Cisco IP phones, including wired and cordless WLAN phones. This solution is for customers with data-connectivity requirements interested in deploying a converged IP telephony solution for up to 96 IP phones. With the Cisco 2800 Series, customers can securely deploy data, voice, and IP telephony on a single platform for their small-to-medium sized branch offices, helping them to streamline their operations and lower their network costs. The Cisco 2800 Series with optional Cisco CME support offers a core set of phone features that customers require for their everyday business needs and takes advantage of the wide array of voice capabilities that are embedded in the Cisco 2800 Series (as shown in Table 1) together with optional features available in Cisco IOS Software to provide a robust IP telephony offering for the small to medium-sized branch-office environment.

Wireless Services

The Cisco 2800 Series can provide a complete wireless solution for branch offices, small/medium sized businesses, and Wi-Fi hotspots. Wireless services enable greater mobility for employees, partners, and customers, resulting in increased productivity. The Cisco 2800 Series supports an integrated access point for wireless LAN connectivity, Wi-Fi Hotspot services for public access, wireless infrastructure services for cordless WLAN telephony and for larger sites, and land mobile radio over IP for radio users.

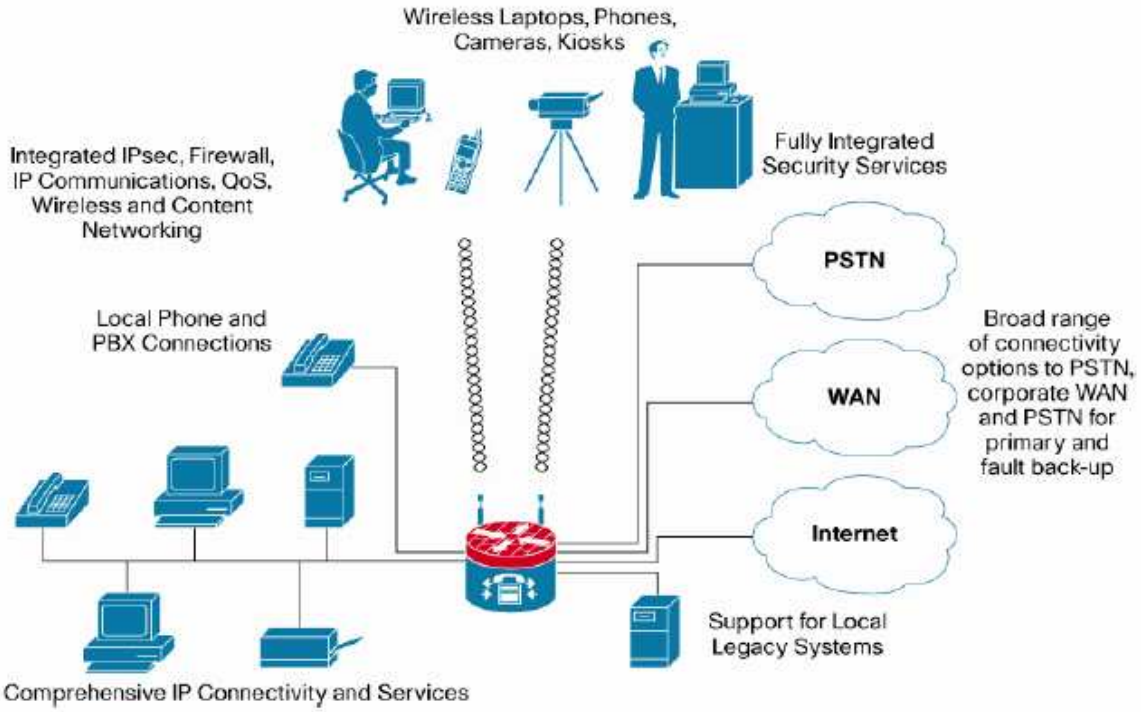
Integrated Services

Figure 2 also highlights the fact that with the unique integrated services architecture of the Cisco 2800 Series, customers can now securely deploy IP Communications with traditional IP routing while leaving interface and module slots available for additional advanced services. With the optional integration of a wide array of services modules, the Cisco 2800 Series offers the ability to easily integrate the functions of standalone network appliances and components into the Cisco 2800 Series chassis itself. Many of these modules, such as the Cisco Network Analysis Module, Cisco Voice Mail Module, Cisco Intrusion Detection Module, Wide Area Application Services Module, and Cisco Content Engine Module, have embedded processors and hard drives that allow them to run largely independently of the router while allowing management from a single management interface. This flexibility greatly expands the potential applications of the Cisco 2800 Series beyond traditional routing while still maintaining the benefits of integration. These benefits include ease of management, lower solution costs (CAPEX and OPEX), and increased speed of deployment.

Applications

Secure Network Connectivity with Converged IP Communications

Figure 2. Secure Network Connectivity with Converged IP Communications



Architecture—Features and Benefits

The Cisco 2800 Series architecture has been designed specifically to meet the expanding requirements of enterprise branch offices and small-to-medium-sized businesses for today's and future applications. The Cisco 2800 Series provides the broadest range of connectivity options in the industry combined with leading-edge availability and reliability features. In addition, Cisco IOS Software provides support for a complete suite of transport protocols, Quality-of-Service (QoS) tools, and advanced security and voice applications for wired and wireless deployments.

Table 1. Architecture—Features and Benefits

Feature	Benefit
Modular Architecture	• A wide variety of LAN and WAN options are available. Network interfaces can be upgraded in the field to accommodate future technologies. • Several types of slots are available to add connectivity and services in the future on an "integrate-as-you-grow" basis. • The Cisco 2800 supports more than 90 modules, including WICs, VICs, network modules, PVDMs, and AIMs (Note: the Cisco 2801 router does not support network modules).
Embedded Security Hardware Acceleration	Each of the Cisco 2800 Series routers comes standard with embedded hardware cryptography accelerators, which when combined with an optional Cisco IOS Software upgrade help enable WAN link security and VPN services.
Integrated Dual Fast Ethernet or Gigabit Ethernet Ports	The Cisco 2800 Series provide two 10/100 on the Cisco 2801 and Cisco 2811 and two 10/100/1000 on the Cisco 2821 and Cisco 2851
Support for Cisco IOS Software	• The Cisco 2800 helps enable end-to-end solutions with full support for the latest Cisco IOS Software-based QoS, bandwidth management, and security features. • Common feature and command set structure across the Cisco 1700, 1800, 2600, 2800, 3700 and 3800 series routers simplifies feature set selection, deployment, management, and training.
Optional Integrated Power Supply for Distribution of Power Over Ethernet (PoE)	An optional upgrade to the internal power supply provides in-line power (802.3af-compliant Power-over-Ethernet [PoE] and Cisco standard inline power) to optional integrated switch modules.
Optional Integrated Universal DC Power Supply	On the Cisco 2811, 2821, and 2851 routers an optional DC power supply is available that extends possible deployments environments such as central offices and industrial environments (Note: not available on the Cisco 2801).
Integrated Redundant-Power-Supply (RPS) Connector	On the Cisco 2811, 2821, and 2851 there is a built in external power-supply connector that eases the addition of external redundant power supply that can be shared with other Cisco products to decrease network downtime by protecting the network components from downtime due to power failures.

Modularity—Features and Benefits

The Cisco 2800 Series provides significantly enhanced modular capabilities (refer to Table 2) while maintaining investment protection for customers. The modular architecture has been redesigned to support increasing bandwidth requirements, time-division multiplexing (TDM) interconnections, and fully integrated power distribution to modules supporting 802.3af PoE or Cisco in-line power, while still supporting most existing modules. With more than 90 modules shared with other Cisco routers such as the Cisco 1700, 1800, 2600, 3700, and 3800 series, interfaces for the Cisco 2800 Series can easily be interchanged with other Cisco routers to provide maximum investment protection in the case of network upgrades. In addition, taking advantage of common interface cards across a network greatly reduces the complexity of managing inventory requirements, implementing large network rollouts, and maintaining configurations across a variety of branch-office sizes.

Table 2. Modularity—Features and Benefits

Feature	Benefit
Enhanced Network-Module (NME) Slots	• The NME slots support existing network modules (Note: NM and NME support on Cisco 2811, 2821, and 2851 only) • NME Slots offer high data throughput capability (up to 1.6Gbps) and support for Power over Ethernet (POE). • NME slots are highly flexible with support for extended NMEs (NME-X on Cisco 2821 and 2851 only) and enhanced double-wide NMEs (NME-XDs) (Note: Cisco 2851 only).
High-Performance WIC (HWIC) Slots with Enhanced Functionality	• Four integrated HWIC slots on Cisco 2811, 2821, and 2851 and two integrated HWIC slots on Cisco 2801 allow for more flexible and dense configurations. • HWICs slots can also support WICs, VICs, and VWICs • HWIC slots offer high data throughput capability (up to 400 Mbps half duplex or 800 Mbps aggregate throughput) and Power over Ethernet (POE) support. • A flexible form factor supports up to two double-wide HWIC (HWIC-D) modules.
Dual AIM Slots	Dual AIM slots support concurrent services such as hardware-accelerated security, ATM segmentation and reassembly (SAR), compression, and voice mail (Refer to Table 7 for

Feature	Benefit
	more details on specific platform support).
Packet Voice DSP Module (PVDM) Slots on Motherboard	Slots for Cisco PVDM2 Modules (DSP Modules) are integrated on the motherboard, freeing slots on the router for other services.
Extension-Voice-Module (EVM) Slot	The EVM supports additional voice services and density without consuming the network-module slot (Note: available only on Cisco 2821 and 2851).
USB Support	Up to two USB ports are available per Cisco 2800 series router. The routers' Universal Serial Bus (USB) ports enable important security and storage capabilities.

Secure Networking—Feature and Benefits

The Cisco 2800 Series features enhanced security functionality as shown in Table 3. Integrated on the motherboard of every Cisco 2800 Series router is hardware-based encryption acceleration that offloads the encryption processes to provide greater IPSec throughput with less overhead for the router CPU when compared with software-based solutions. With the integration of optional VPN modules (for enhanced VPN tunnel count), Cisco IOS Software-based firewall, network access control, or content-engine network modules, Cisco offers the industry's most robust and adaptable security solution for branch-office routers.

Table 3. Secure Networking—Feature and Benefits

Feature	Benefit
Cisco IOS Software Firewall	Sophisticated security and policy enforcement provides features such as stateful, application-based filtering (context-based access control), per-user authentication and authorization, real-time alerts, transparent firewall, and IPv6 firewall.
Secure Sockets Layer (SSL)	SSL provides security for web transactions by handling authentication, data enryption and digital signatures. The 2800 Series supports SSL VPNs and SSL acceleration via the AIM-VPN/SSL-3.
Onboard VPN Encryption Acceleration	The Cisco 2800 Series supports IPSec Digital Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES) 128, AES 192, and AES 256 cryptology without consuming an AIM slot.
Network Admissions Control (NAC)	A Cisco Self-Defending Network initiative, NAC seeks to dramatically improve the ability of networks to identify, prevent, and adapt to threats by allowing network access only to compliant and trusted endpoint devices.
Multiprotocol Label Switching (MPLS) VPN Support	The Cisco 2800 Series supports specific provider edge functions plus a mechanism to extend customers' MPLS VPN networks out to the customer edge with virtual routing and forwarding (VRF) firewall and VRF IPSec. For details on the MPLS VPN support on the different versions of the Cisco 2800 Series, please check the feature navigator tool on http://www.cisco.com.
USB eToken Support	USB eTokens from Aladdin Knowledge Systems (available at http://www.aladdin.com/etoken/cisco/) provides secure configuration distribution and allows users to store VPN credentials for deployment
AIM-Based Security Acceleration	Support for an optional dedicated security AIM can deliver 2 to 3 times the performance of embedded encryption capabilities with Layer 3 compression.
Intrusion Prevention System (IPS)	Flexible and high performance support is offered through Cisco IOS® Software or an intrusion-detection-system (IDS) network module. The ability to load and enable selected IDS signatures in the same manner as Cisco IDS Sensor Appliances
Advanced Application Inspection and Control	Cisco IOS Firewall includes HTTP and several email inspection engines that can be used to detect misuse of port 80 and email connectivity.
Cisco Easy VPN Remote and Server Support	The Cisco 2800 Series eases administration and management of point-to-point VPNs by actively pushing new security policies from a single headend to remote sites.
Dynamic Multipoint VPN (DMVPN)	DMVPN is a Cisco IOS Software solution for building IPSec + generic routing encapsulation (GRE) VPNs in an easy and scalable manner.
Group Encrypted Transport (GET) VPN	GET VPN is a Cisco IOS Software solution that simplifies securing large Layer 2 or MPLS networks requiring partial or full-mesh connectivity by providing tunnel-less VPN connectivity.
URL Filtering	URL filtering is available onboard with an optional content-engine network module or external with a PC server running the URL filtering software.
Cisco Router and Security Device Manager (SDM)	This intuitive, easy-to-use, Web-based device-management tool is embedded within the Cisco IOS Software access routers; it can be accessed remotely for faster and easier deployment of Cisco routers for both WAN access and security features.

IP Telephony Support—Features and Benefits

The Cisco 2800 Series allows network managers to provide scalable analog and digital telephony without investing in a one-time solution (refer to Table 4 for more detail), allowing enterprises greater control of their converged telephony needs. Using the voice and fax modules, the Cisco 2800 Series can be deployed for applications ranging from voice-over-IP (VoIP) and voice-over-Frame Relay (VoFR) transport to robust, centralized solutions using the Cisco Survivable Remote Site Telephony (SRST) solution or distributed call processing using Cisco Call Manager Express (CME). The architecture is highly scalable with the ability to connect up to 12 T1/E1s trunks, 52 foreign-exchange-station (FXS) ports, or 36 foreign-exchange-office (FXO) ports.

Table 4. IP Telephony Support—Features and Benefits

Feature	Benefit
IP Phone Support	Optional support for Cisco in-line power distribution to Ethernet switch network modules and HWICs can be used to power Cisco IP phones.
EVM Module Slots	Extension Voice Module Slots, available only on the Cisco 2821 and Cisco 2851, provide support for the Cisco High-Density Analog and Digital Extension Module for Voice and Fax, providing support for up to 24 total voice and fax sessions without consuming a Network Module Slot.
PVDM (DSP) Slots on Motherboard	DSP (PVDM2) modules deliver support for analog and digital voice, conferencing, transcoding, and secure Real-Time Transport Protocol (RTP) applications.
Integrated Call Processing	Cisco CME is an optional solution embedded in Cisco IOS Software that provides call processing for Cisco IP phones. Cisco CME delivers telephony features similar to those that are commonly used by business users to meet the requirements of the small to medium-sized offices.
Integrated Voice Mail	Support for up to a 250 mailboxes using the Cisco Unity® Express voice messaging system is possible with the integration of an optional voice-mail AIM or network module.
Broad Range of Voice Interfaces	Interfaces for public switched telephone network (PSTN), private branch exchange (PBX), and key system connections include FXS; FXO; analog direct inward dialing (DID); ear and mouth (E&M); Centralized Automated Message Accounting (CAMA); ISDN Basic Rate Interface (BRI); and T1, E1, and J1 with ISDN Primary Rate Interface (PRI); QSIG; E1 R2; and several additional channel-associated-signaling (CAS) signaling schemes.
Survivable Remote Site Telephony (SRST)	Branch offices can take advantage of centralized call control while cost-effectively providing local branch backup using SRST redundancy for IP telephony.

Wireless Support—Features and Benefits

The Cisco 2800 Series can provide a complete wireless solution for branch offices, small/medium sized businesses, and Wi-Fi hotspots. Wireless services enable greater mobility for employees, partners, and customers, resulting in increased productivity.

Table 5. Wireless Support—Features and Benefits

Feature	Benefit
WLAN Connectivity	• The 802.11b/g or 802.11a/b/g HWIC access point interface card can be used to provide integrated WLAN connectivity to mobile clients at sites requiring a single access point, resulting in mobility and enhanced productivity for users. • Dual RP-TNC connectors enable diversity and allow for optimum coverage through the use of external antennas.
Wireless Infrastructure Services	• Telephony support for wired and WLAN IP phones is delivered by Cisco CallManager Express (CCME) or by Survivable Remote Site Telephony (SRST) with Cisco CallManager. Cordless WLAN IP phones allow users to be mobile and more productive. • Integrated switch modules with Power over Ethernet (POE) enable support for Cisco Aironet access points (for larger sites) as well as wired IP phones. • Mobility for clients from WLAN to cellular networks is enabled by Mobile IP home agent support. • IEEE 802.1x local authentication using LEAP provides enhanced reliability through survivable authentication for WLAN clients during WAN failures. • Customizable guest access is enabled with the service selection gateway features, along with the Subscriber Edge Services Manager.

Feature	Benefit
Land Mobile Radio Over IP	LMR over IP support allows radio users (e.g., security personnel, maintenance personnel, police officers, etc.) to communicate via IP with phone and PC users, delivering improved communications and productivity.
Wi-Fi Hotspot Services	The access zone router and service selection gateway services features can be used to deploy secure public WLAN access services with an integrated HWIC-AP for small sites or with Cisco Aironet access points for larger sites. Wi-Fi hotspot services can be offered for additional revenue for public locations (e.g., restaurants, hotels, airports, etc.) or a value-added service for customer satisfaction.

Cost of Ownership and Ease of Use—Features and Benefits

The Cisco 2800 Series continues the heritage of offering versatility, integration, and power to branch offices. The Cisco 2800 Series offers many enhancements to help enable the support of multiple services in the branch office as shown in the table below.

Table 6. Cost of Ownership and Ease of Use—Feature and Benefits

Feature	Benefit
Integrated Channel Service Unit/Data Service Unit (CSU/DSU), Add/Drop Multiplexers, Firewall, Modem, Compression, and Encryption	Consolidates typical communications equipment found in branch-office wiring closets into a single, compact unit; this space-saving solution provides better manageability
Optional Network Analysis Module	Provides application-level visibility into network traffic for troubleshooting, performance monitoring, capacity planning, and managing network-based services (Note: Cisco 2811, 2821, and 2851 only)
Cisco IOS IP Service Level Agreements (IP SLAs)	With Cisco IOS IP SLAs, users can verify service guarantees, increase network reliability by validating network performance, proactively identify network issues, and increase Return on Investment (ROI) by easing the deployment of new IP services
Cisco IOS Software Warm Reboot	Reduces system boot time, and decreases downtime caused by Cisco IOS Software reboots (Cisco 2811, 2821 and 2851)
Enhanced Setup Feature	Optional setup wizard with context-sensitive questions guides the user through the router configuration process, allowing faster deployment
CiscoWorks Support	Offers advanced management and configuration capabilities through a Web-based GUI
Cisco AutoInstall	Configures remote routers automatically across a WAN connection to save cost of sending technical staff to the remote site
Cisco IOS Embedded Event Manager (EEM)	Enables automation of many network management tasks and directs the operation of Cisco IOS to increase availability, collect information, and notify external systems or personnel about critical events

Summary and Conclusion

As companies strive to lower the cost of running their network and increase the productivity of their end users with network applications, more intelligent branch-office solutions are required. The Cisco 2800 Series offers these solutions by providing enhanced performance and increased modular density to support multiple services at wire speed. The Cisco 2800 Series is designed to consolidate the functions of many separate devices into a single, compact package that can be managed remotely. Because the Cisco 2800 Series routers are modular devices, interface configurations are easily customized to accommodate a wide variety of network applications, such as branch-office data access, integrated switching, voice and data integration, wireless LAN services, dial access services, VPN access and firewall protection, business-class DSL, content networking, intrusion prevention, inter-VLAN routing, and serial device concentration. The Cisco 2800 Series provides customers with the industry's most flexible, adaptable infrastructure to meet both today's and tomorrow's business requirements for maximum investment protection.

Product Specifications

Table 7. Chassis Specifications

Cisco 2800 Series	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
Product Architecture				
DRAM	• Default: 128 MB • Maximum: 384 MB	• Default: 256 MB • Maximum: 768 MB	• Default: 256 MB • Maximum: 1 GB	
Compact Flash	• Default: 64 MB • Maximum: 128MB	• Default: 64 MB • Maximum: 256 MB		
Fixed USB 1.1 Ports	1	2		
Onboard LAN Ports	2-10/100		2-10/100/1000	
Onboard AIM (Internal) Slot	2			
Interface Card Slots	• 4 slots; 2 slots support HWIC, WIC, VIC, or VWIC type modules • 1 slot supports WIC, VIC, or VWIC type modules • 1 slot supports VIC or VWIC type modules	4 slots, each slot can support HWIC, WIC, VIC, or VWIC type modules		
Network-Module Slot	No	1 slot, supports NM and NME type modules	1 slot, supports NM, NME and NME-X type modules	1 slot, supports NM, NME, NME-X, NMD and NME-XD type modules
Extension Voice Module Slot	0		1	
PVDM (DSP) Slots on Motherboard	2		3	
Integrated Hardware-Based Encryption	Yes			
VPN Hardware Acceleration (on Motherboard)	DES, 3DES, AES 128, AES 192, and AES 256			
Optional Integrated In-Line Power (PoE)	Yes, requires AC-IP power supply			
Console Port (up to 115.2 kbps)	1			
Auxiliary Port (up to 115.2 kbps)	1			
Minimum Cisco IOS Software Release	12.3(8)T			
Rack Mounting	Yes, 19-inch	Yes, 19- and 23-in. options		
Wall Mounting	No	Yes	No	No
Power Requirements				
AC Input Voltage	100 to 240 VAC, autoranging			
AC Input Frequency	47-63 Hz			
AC Input Current	2A (110V) 1A (230V)		3A (110V) 2A (230V)	
AC Input Surge Current	50A maximum, one cycle (-48V power included)			

Cisco 2800 Series	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
AC-IP Maximum In-Line Power Distribution	120W	160W	240W	360W
AC-IP Input Current	4A (110V) 2A (230V)		8A (110V) 4A (230V)	
AC-IP Input Surge Current	50A maximum, one cycle (-48V power included)			
DC Input Voltage	No DC Power Option available	24 to 60 VDC, autoranging positive or negative		
DC Input Current	• No DC Power Option available	• 8A (24V) • 3A (60V) • Startup current 50A<10 ms	• 12A (24V) • 5A (60V) • Startup current 50A<10 ms	
Power Dissipation-AC without IP Phone Support	150W (511 BTU/hr)	170W (580 BTU/hr)	280W (955 BTU/hr)	280W (955 BTU/hr)
Power Dissipation-AC with IP Phone Support-System Only	150W (511 BTU/hr)	210W (717 BTU/hr)	310W (1058 BTU/hr)	370W (1262 BTU/hr)
Power Dissipation-AC with IP Phone Support-IP Phones	180W (612 BTU/hr)	160W (546 BTU/hr)	240W (819 BTU/hr)	360W (1128 BTU/hr)
Power Dissipation-DC	Not applicable	180W (614 BTU/hr)	300W (1024 BTU/hr)	300W (1024 BTU/hr)
RPS	No	External only, connector for RPS provided by default		
Recommended RPS Unit	No RPS option	Cisco RPS-675 Redundant Power System		
Environmental Specifications				
Operating Temperature	32° to 104°F (0° to 40°C)			
Non-Operating Temperature	4° to 149°F (-20° to 65°C)			
Maximum Operating Temperature at Altitude	• 40°C @ sea level • 31°C @ 6,000 ft (1800 m) • 25°C @ 10,000 ft (3000 m) Note: Derate 1.5°C per 1000 ft	• 40°C @ sea level • 40°C @ 6,000 ft (1800 m) • 30°C @ 13,000 ft (4000 m) • 27.2°C @ 15,000 ft (4600 m) Note: Derate 1.4°C per 1,000 ft above 6,000 ft		
Operating Humidity	10 to 85% non-condensing	5 to 95%, non-condensing		
Dimensions (H x W x D)	• 1.72 x 17.5 x 16.5 in. • (43.7 x 445 x 419 mm)	• 1.75 x 17.25 x 16.4 in. • (44.5 x 438.2 x 416.6 mm)	• 3.5 x 17.25 x 16.4 in. • (88.9 x 438.2 x 416.6 mm)	
Rack Height	1 rack unit (1RU)		2RU	
Weight (Fully Configured)	13.7 lb (6.2 kg)	14 lb (6.4 kg)	25 lb (11.4 kg)	
Noise Level (Min/Max)	• 39 dBA for normal operating temperature (<90°F/32.2°C) • 53.5 dBA (@ maximum fan speed)	• 47 dBA for normal operating temperature (<90°F/32.2°C) • 57 dBA (@ maximum fan speed)	• 44 dBA for normal operating temperature (<90°F/32.2°C) • 53 dBA (@ maximum fan speed)	
Regulatory Compliance				
NEBS	No	Yes	Yes	

Cisco 2800 Series	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
Safety	• UL 60950 • CAN/CSA C22.2 No. 60950 • IEC 60950 • EN 60950-1 • AS/NZS 60950			
Immunity	• EN300386 • EN55024/CISPR24 • EN50082-1 • EN61000-6-2			
EMC	• FCC Part 15 • ICES-003 Class A • EN55022 Class A • CISPR22 Class A • AS/NZS 3548 Class A • VCCI Class A • EN 300386 • EN61000-3-3 • EN61000-3-2			
FIPS-2	FIPS 140-2 Certification for 2801, 2811, 2821, 2851			
TELCOM**	• For all four platforms, Telecom compliance standards depend upon country and interface type. Interfaces comply with FCC Part 68, CS-03, JATE Technical Conditions, European Directive 99/5/EC and relevant TBR's. For specific information see the datasheet for the specific interface card. • Homologation requirements vary by country and interface type. For specific country information, see the on-line approvals data base: http://tools.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH&module=EXTERNAL_SEARCH			

Modular Support

Table 8. Modules and Interface Cards Supported

Module	Description	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
Ethernet Switching Network Modules					
NME-16ES-1G	One 16-port 10/100 EtherSwitch service module, 1 10/100/1000 port, and IP Base	No	X	X	X
NME-16ES-1G-P	One 16-port 10/100 Cisco EtherSwitch service module with802.3af, 1 10/100/1000 port, and IP Base	No	X	X	X
NME-X-23ES-1G	One 23-port 10/100 EtherSwitch service module, 1 10/100/1000 port, and IP Base	No	No	X	X
NME-X-23ES-1G-P	One 23-port 10/100 Cisco EtherSwitch service module with802.3af, 1 10/100/1000 port with 802.3af, and IP Base	No	No	X	X
NME-XD-24ES-2S-P	One 24-port 10/100 Cisco EtherSwitch service module with802.3af, 1 SFP, Cisco StackWise connectors, and IP Base	No	No	No	X
NME-XD-48ES-2S-P	One 48-port 10/100 Cisco EtherSwitch service module with 802.3af, 2 SFPs, and IP Base	No	No	No	X
NM-16ESW	16-port 10/100 Cisco EtherSwitch® Network Module	No	X	X	X
NM-16ESW-1GIG	16-port 10/100 Cisco EtherSwitch Network Module with 1 Gigabit Ethernet (1000BASE-T) port	No	X	X	X

Module	Description	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
NM-16ESW-PWR	16-port 10/100 Cisco EtherSwitch Network Module with in-line power support	No	X	X	X
NM-16ESW-PWR-1GIG	16-port 10/100 Cisco EtherSwitch Network Module with in-line power and Gigabit Ethernet	No	X	X	X
NMD-36ESW	36-port 10/100 Cisco EtherSwitch High-Density Services Module (HDSM)	No	No	No	X
NMD-36ESW-2GIG	36-port 10/100 Cisco EtherSwitch HDSM with 1 Gigabit Ethernet (1000BASE-T) port	No	No	No	X
NMD-36ESW-PWR	36-port 10/100 Cisco EtherSwitch HDSM with in-line power support	No	No	No	X
NMD-36ESW-PWR-2G	36-port 10/100 Cisco EtherSwitch HDSM with in-line power and Gigabit Ethernet	No	No	No	X
Serial Connectivity Network Modules					
NM-1T3/E3	1-port clear-channel T3/E3 network module	No	X	X	X
NM-1HSSI	1-port High-Speed Serial Interface (HSSI) network module	No	X	X	X
NM-4A/S	4-port asynchronous/synchronous serial network module	No	X	X	X
NM-8A/S	8-port asynchronous/synchronous serial network module	No	X	X	X
NM-16A/S	16-port asynchronous/synchronous serial network nodule	No	X	X	X
NM-16A	16-port asynchronous serial network module	No	X	X	X
NM-32A	32-port asynchronous serial network module	No	X	X	X
Channelized T1/E1 and ISDN Network Modules					
NM-1CE1T1-PRI	1-port Channelized E1/T1/ISDN PRI network module	No	X	X	X
NM-2CE1T1-PRI	2-port Channelized E1/T1/ISDN PRI network module	No	X	X	X
NM-4B-S/T	4-port ISDN BRI network module (S/T interface)	No	X	X	X
NM-4B-U	4-port ISDN BRI network module with integrated Network Termination 1 (NT1) (U interface)	No	X	X	X
NM-8B-S/T	8-port ISDN BRI network module (S/T interface)	No	X	X	X
NM-8B-U	8-port ISDN BRI network module with integrated NT1 (U interface)	No	X	X	X
ATM Network Modules					
NM-1A-T3	1-port DS-3 ATM network module	No	X	X	X
NM-1A-E3	1-port E3 ATM network module	No	X	X	X
Analog Dialup and Remote Access Network Modules					
NM-8AM-V2	8-port analog modem network module with v.92	No	X	X	X
NM-16AM-V2	16-port analog modem network module with v.92	No	X	X	X
Voice Network Modules and Accessories					
NM-HD-1V	1-slot IP Communications voice and fax network module	No	X	X	X

Module	Description	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
NM-HD-2V	2-slot IP Communications voice and fax network module	No	X	X	X
NM-HD-2VE	2-slot IP Communications enhanced voice and fax network module	No	X	X	X
NM-HDA-4FXS	High-density analog voice and fax network module with 4 FXS slots	No	X	X	X
NM-HDV2	IP Communications high-density voice and fax network module	No	X	X	X
NM-HDV2-1T1/E1	1-port T1/E1 IP Communications high-density voice and fax network module	No	X	X	X
NM-HDV2-2T1/E1	2-port T1/E1 IP Communications high-density voice and fax network module	No	X	X	X
NM-HDV=	High Density Voice/Fax Network Module (Single VIC Slot)	No	X	X	X
NM-HDV-1T1-12	1-port 12-channel T1 voice and fax network module	No	X	X	X
NM-HDV-1T1-24	1-port 24-channel T1 voice and fax network module	No	X	X	X
NM-HDV-1T1-24E	Single-port 24 enhanced channel T1 voice and fax network module	No	X	X	X
NM-HDV-2T1-48	2-port 48-channel T1 voice and fax network module	No	X	X	X
NM-HDV-1E1-12	1-port 12-channel E1 voice and fax network module	No	X	X	X
NM-HDV-1E1-30	1-port 30-channel E1 voice and fax network module	No	X	X	X
NM-HDV-1E1-30E	1-port 30-enhanced-channel E1 voice and fax Network Module	No	X	X	X
NM-HDV-2E1-60	2-port 60-channel E1 voice and fax network module	No	X	X	X
NM-HDV-1J1-30	1-port 30-channel J1 high-density voice network module	No	X	X	X
NM-HDV-1J1-30E	1-port 30-enhanced-channel J1 high-density voice network module	No	X	X	X
NM-HDV-FARM-C36	36-port transcoding and conferencing DSP farm	No	X	X	X
NM-HDV-FARM-C54	54-port transcoding and conferencing DSP farm	No	X	X	X
NM-HDV-FARM-C90	90-port transcoding and conferencing DSP farm	No	X	X	X
Application Network Modules					
NME-WAE-302-K9	Cisco Wide Area Application Services (WAAS) Network Module with 80 GB hard disk and 512 MB memory	No	X	X	X
NME-WAE-502-K9	Cisco Wide Area Application Services (WAAS) Network Module with 120 GB hard disk and 1 GB memory	No	X	X	X
NME-AON-K9	Cisco 2800/3700/3800 Series AON Enhanced Network Module	No	X	X	X
NM-CE-BP-40G-K9	Cisco Content Engine Network Module, basic performance, 40-GB IDE hard disk	No	X	X	X
NM-CE-BP-80G-K9	Cisco Content Engine Network Module, basic performance, 80-GB IDE hard disk	No	X	X	X

Module	Description	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
NM-CE-BP-40G-S-K9	Cisco Content Engine Network Module for Security, basic performance, 40-GB IDE hard disk	No	X	X	X
NM-CE-BP-80G-S-K9	Cisco Content Engine Network Module for Security, basic performance, 80-GB IDE hard disk	No	X	X	X
NM-CIDS-K9	Cisco IDS Network Module	No	X	X	X
NM-CUE	Cisco Unity Express Voice-Mail Network Module	No	X	X	X
NM-CUE-EC	Cisco Unity Express Voice-Mail Network Module extended capacity	No	X	X	X
NM-NAM	Cisco 2600, 3660, and 3700 series network analysis module	No	X	X	X
NM-AIR-WLC6-K9	Cisco wireless LAN controller network module	No	X	X	X
Circuit Emulation over IP (CEoIP) Network Modules					
NM-CEM-4SER	4-port serial Circuit Emulation over IP (CEoIP) network module	No	X	X	X
NM-CEM-4TE1	4-port T1/E1 Circuit Emulation over IP (CEoIP) network module	No	X	X	X
Satellite Module					
NM-1VSAT-GILAT	Cisco IP VSAT Satellite WAN Network Module	No	X	X	X
Extension Voice Modules					
EVM-HD-8FXS/DID	High density voice/fax extension module -8 FXS/DID	No	No	X	X
Ethernet Switching High-Speed WAN Interface Cards					
HWIC-4ESW	4-port single-wide 10/100BaseT Ethernet switch HWIC	X	X	X	X
HWIC-D-9ESW	9-port double-wide 10/100BaseT Ethernet switch HWIC	X	X	X	X
HWIC-4ESW-POE	4-port Ethernet switch HWIC, Power over Ethernet capable	X	X	X	X
HWIC-D-9-ESW-POE	9-port Ethernet switch HWIC, Power over Ethernet capable	X	X	X	X
Ethernet High-Speed WAN Interface Cards					
HWIC-1FE	1-port Fast Ethernet HWIC	X	X	X	X
HWIC-1GE-SFP	Cisco Gigabit Ethernet High-Speed Interface Card	No	X	X	X
Wireless High-Speed WAN Interface Cards					
HWIC-AP-G-A HWIC-AP-G-E HWIC-AP-G-J	802.11b/g HWIC access point interface card (A-Americas; E-Europe; J-Japan)	X	X	X	X
HWIC-AP-AG-A HWIC-AP-AG-E HWIC-AP-AG-J	802.11a/b/g HWIC access point interface card (A-Americas; E-Europe; J-Japan)	X	X	X	X
Serial WAN Interface Cards and High-Speed WAN Interfaced Cards					
HWIC-4T	4-Port serial HWIC	X	X	X	X
HWIC-4A/S	4-Port Async/Sync serial HWIC	X	X	X	X
HWIC-8A	8-Port Async HWIC	X	X	X	X
HWIC-8A/S-232	8-Port Async/Sync serial HWIC, EIA-232	X	X	X	X
HWIC-16A	16-Port Async HWIC	X	X	X	X
WIC-1T	1-port high-speed serial WIC	X	X	X	X

Module	Description	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
WIC-2T	2-port high-speed serial WIC	X	X	X	X
WIC-2A/S	2-port Asynch/Synch serial WIC	X	X	X	X
CSU/DSU WAN Interface Cards					
WIC-1DSU-T1-V2	1-port T1/Fractional-T1 DSU/CSU WIC	X	X	X	X
WIC-1DSU-56K4	1-port 4-wire 56-/64-kbps CSU/DSU WIC	X	X	X	X
ISDN BRI WAN Interface Cards					
WIC-1B-U-V2	1-port ISDN BRI with integrated NT1 (U interface)	X	X	X	X
WIC-1B-S/T-V3	1-port ISDN BRI with S/T interface	X	X	X	X
DSL WAN Interface Cards					
HWIC-1ADSL	1-port ADSLoPOTS HWIC	X	X	X	X
HWIC-1ADSLI	1-port ADSLoISDN HWIC	X	X	X	X
HWIC-ADSL-B/ST	2-port HWIC with 1-port ADSLoPOTS and 1-port ISDN BRI-S/T	X	X	X	X
HWIC-ADSLI-B/ST	2-port HWIC with 1-port ADSLoISDN and 1-port ISDN BRI-S/T	X	X	X	X
HWIC-2SHDSL	2-port G.SHDSL HWIC with 2-wire and 4-wire support	X	X	X	X
HWIC-4SHDSL	4-port G.SHDSL HWIC with 2-wire, 4-wire, and 8-wire support	X	X	X	X
WIC-1ADSL	1-port asymmetric DSL (ADSL) over POTS service WIC	X	X	X	X
WIC-1ADSL-DG	1-port ADSL over basic telephone service with dying-gasp WIC	X	X	X	X
WIC-1ADSL-I-DG	1-port ADSL over ISDN with dying-gasp WIC	X	X	X	X
WIC-1SHDSL	1-port G.SHDSL WIC (2-wire only)	X	X	X	X
WIC-1SHDSL-V2	1-port G.SHDSL WIC (2-wire or 4-wire)	X	X	X	X
WIC-1SHDSL-V3	1-port G.SHDSL WIC with 4-wire support	X	X	X	X
Cable (DOCSIS-qualified) High-Speed WAN Interfaced Cards					
HWIC-CABLE-D-2	1-port DOCSIS 2.0 qualified cable HWIC	X	X	X	X
HWIC-CABLE-E/J-2	1-port Euro/J-DOCSIS 2.0 qualified cable HWIC	X	X	X	X
T1, E1, and G.703 Multiflex Trunk Voice Cards and WAN Interface Cards					
VWIC2-1MFT-T1/E1	1-Port T1/E1 Voice/WAN with Drop & Insert	X	X	X	X
VWIC2-2MFT-T1/E1	2-Port T1/E1 Voice/WAN with Drop & Insert	X	X	X	X
VWIC2-1MFT-G703	1-Port T1/E1 Voice/WAN with D&I & unstructured E1 (G703)	X	X	X	X
VWIC2-2MFT-G703	2-Port T1/E1 Voice/WAN with D&I & unstructured E1 (G703)	X	X	X	X
VWIC-2MFT-T1-DI	2-port RJ-48 multiflex trunk-T1 with drop and insert	X	X	X	X
VWIC-2MFT-T1	2-port RJ-48 multiflex trunk-T1	X	X	X	X
VWIC-1MFT-T1	1-port RJ-48 multiflex trunk-T1	X	X	X	X
VWIC-1MFT-E1	1-port RJ-48 multiflex trunk-E1	X	X	X	X
VWIC-1MFT-G703	1-port RJ-48 multiflex trunk-G.703	X	X	X	X

Module	Description	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
VWIC-2MFT-E1	2-port RJ-48 multiflex trunk-E1	X	X	X	X
VWIC-2MFT-E1-DI	2-port RJ-48 multiflex trunk-E1 with drop and insert	X	X	X	X
VWIC-2MFT-G703	2-port RJ-48 multiflex trunk-G.703	X	X	X	X
Voice Interface Cards					
VIC2-2FXS	2-port VIC-FXS	X	X	X	X
VIC2-2FXO	2-port VIC-FXO (universal)	X	X	X	X
VIC2-4FXO	4-port VIC-FXO (universal)	X	X	X	X
VIC2-2E/M	2-port VIC-E&M	X	X	X	X
VIC2-2BRI-NT/TE	2-port VIC card-BRI (NT and TE)	X	X	X	X
VIC-2DID	2-port DID voice and fax interface card	X	X	X	X
VIC-4FXS/DID	4-port FXS or DID VIC	X	X	X	X
Analog Modem WAN Interface Cards					
WIC-1AM	1-port analog modem WIC	X	X	X	X
WIC-2AM	2-port analog modem WIC	X	X	X	X
WIC-1AM-V2	1-port analog modem WIC (updated version)	X	X	X	X
WIC-2AM-V2	2-port analog modem WIC (updated version)	X	X	X	X
Advanced Integration Modules					
AIM-ATM	High-performance ATM SAR AIM	No	X	X	X
AIM-ATM-1E1	High Performance ATM AIM/E1 Bundle, AIM-ATM with VWIC-1MFT-E1	No	X	X	X
AIM-ATM-1T1	High Performance ATM AIM/T1 Bundle, AIM-ATM with VWIC-1MFT-T1	No	X	X	X
AIM-ATM-1T1/E1	T1/E1 ATM bundle includes 1 VWIC2-1MFT-T1/E1 and 1 AIM-ATM.	No	X	X	X
AIM-ATM-4T1/E1	T1/E1 ATM bundle includes 2 VWIC2-2MFT-T1/E1s and 1 AIM-ATM.	No	X	X	X
AIM-ATM-4T1/E1	4 port ATM IMA bundle	No	X	X	X
AIM-ATM-4T1/E1	4 port ATM IMA bundle	No	X	X	X
AIM-COMPR2-V2	Data compression AIM	No	X	X	X
AIM-CUE	Cisco Unity Express Voice-Mail AIM	X	X	X	X
AIM-VPN/SSL-2	DES/3DES/AES/SSL VPN Encryption/Compression Advanced Integration Module (AIM) with IPv6 encryption.	X	X	X	X
AIM-VPN/EPII-PLUS	Enhanced-performance DES, 3DES, AES, and compression VPN encryption AIM	X	X	X	X
Packet Voice/Data Modules					
PVDM2-8	8-channel fax and voice DSP module	X	X	X	X
PVDM2-16	16-channel fax and voice DSP module	X	X	X	X
PVDM2-32	32-channel fax and voice DSP module	X	X	X	X
PVDM2-48	48-channel fax and voice DSP module	X	X	X	X
PVDM2-64	64-channel fax and voice DSP module	X	X	X	X
Digital Modem Packet Voice/Data Modules					
PVDM2-12DM	12 Port Digital Modem Module	No	X	X	X
PVDM2-24DM	24 Port Digital Modem Module	No	X	X	X

Module	Description	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
PVDM2-36DM	36 Port Digital Modem Module	No	X	X	X
USB Flash Storage					
MEMUSB-64FT	64 Mb USB Flash	X	X	X	X
MEMUSB-128FT	128 Mb USB Flash	X	X	X	X
MEMUSB-256FT	256 Mb USB Flash	X	X	X	X

Availability

The Cisco 2800 Series has been orderable since September, 2004, with first customer shipments at the end of September 2004.

Ordering Information

To place an order, visit the Cisco Ordering Home Page.

Table 9. Ordering Information for Cisco 2800 Integrated Services Routers

Part Number	Product Name
CISCO2801	Integrated services router with AC power, 2FE, 4 Interface Card Slots, 2 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
CISCO2801-AC-IP	Integrated services router with AC power including power over ethernet distribution capability, 2FE, 4 Interface Card Slots, 2 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
CISCO2811	Integrated services router with AC power, 2FE, 1 NME, 4 HWICs, 2 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
CISCO2811-AC-IP	Integrated services router with AC power including power over ethernet distribution capability, 2FE, 1 NME, 4 HWICs, 2 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
CISCO2811-DC	Integrated services router with DC power, 2FE, 1 NME, 4 HWICs, 2 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
CISCO2821	Integrated services router with AC power, 2GE, 1 NME-X, 1 EVM, 4 HWICs, 3 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
CISCO2821-AC-IP	Integrated services router with AC power including power over ethernet distribution capability, 2GE, 1 NME-X, 1 EVM, 4 HWICs, 3 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
CISCO2821-DC	Integrated services router with DC power, 2GE, 1 NME-X, 1 EVM, 4 HWICs, 3 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
CISCO2851	Dual Gigabit Ethernet integrated services router with AC power, 2GE, 1 NME-XD, 1 EVM, 4 HWICs, 3 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
CISCO2851-AC-IP	Integrated services router with AC power including power over ethernet distribution capability, 2GE, 1 NME-XD, 1 EVM, 4 HWICs, 3 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
CISCO2851-DC	Integrated services router with DC power, 2GE, 1 NME-XD, 1 EVM, 4 HWICs, 3 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software

Also, check with your Cisco representative regarding security, xDSL, and voice bundles for the Cisco 2800 Series.

To download the software, visit the Cisco Software Center.

Table 10. Software Ordering Information

Part Number	Product Name	Supported Platform
S28IPB	Cisco 2800 IP Base	Cisco 2801
S28NIPBK9	Cisco 2800 IP Base K9	Cisco2801
S28IPV	Cisco 2800 IP Voice	Cisco 2801
S28NIPVK9	Cisco 2800 IP Voice K9	Cisco 2801
S28ASK9	Cisco 2800 Advanced Security K9	Cisco 2801
S28EB	Cisco 2800 Enterprise Base	Cisco 2801

Part Number	Product Name	Supported Platform
S280EBK9	Cisco 2800 Enterprise Base K9	Cisco 2801
S28SPSK9	Cisco 2800 SP Services K9	Cisco 2801
S280ES	Cisco 2800 Enterprise Services without Crypto	Cisco 2801
S28ESK9	Cisco 2800 Enterprise Services K9	Cisco 2801
S28AISK9	Cisco 2800 Advanced IP Services K9	Cisco 2801
S28AESK9	Cisco 2800 Advanced Enterprise Services K9	Cisco 2801
S28NIPB	Cisco 2800 IP Base	Cisco 2811, 2821, 2851
S28NIPV	Cisco 2800 IP Voice	Cisco 2811, 2821, 2851
S28NIVS	Cisco 2800 Int Voice/Video: GK, IPIP GW, TDMIP GW	Cisco 2811, 2821, 2851
S28NAVSK9	Cisco 2800 Int Voice/Video: GK, IPIP. GW, TDMIP GW AES	Cisco 2811, 2821, 2851
S28NASK9	Cisco 2800 Advanced Security K9	Cisco 2811, 2821, 2851
S28NEB	Cisco 2800 Enterprise Base	Cisco 2811, 2821, 2851
S28NEBK9	Cisco 2800 Enterprise Base K9	Cisco 2811, 2821, 2851
S28NSPSK9	Cisco 2800 SP Services K9	Cisco 2811, 2821, 2851
S28NES	Cisco 2800 Enterprise Services	Cisco 2811, 2821, 2851
S28NESK9	Cisco 2800 Enterprise Services K9	Cisco 2811, 2821, 2851
S28NAISK9	Cisco 2800 Advanced IP Services K9	Cisco 2811, 2821, 2851
S28NAESK9	Cisco 2800 Advanced Enterprise Services K9	Cisco 2811, 2821, 2851
S28NSNAK9	Cisco 2800 Advanced Enterprise Services with SNA switching software	Cisco 2811, 2821, 2851

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power of your business. For more information about Cisco Services, see Cisco Technical Support Services or Cisco Advanced Services.

For More Information

For more information about the Cisco 2800 Series, visit http://www.cisco.com/en/US/products/hwithrouters/ or contact your local account representative.

Anexo 2:

Configuración de protocolos de enrutamiento en XORP

ANEXO 2: CONFIGURACION DE PROTOCOLOS DE ENRUTAMIENTO EN XORP

Chapter 2

Configuration Overview

2.1 Introduction

A XORP router must be configured to perform the desired operations. The configuration information can be provided in one of the two ways:

- Use a configuration file when the xorp_rtrmgr is started. By default, the xorp_rtrmgr will load the configuration from file "config.boot" in the XORP installation directory. This file can be specified by the "-b <filename>" command line option:

  ```
  xorp_rtrmgr -b my_config.boot
  ```

  See "rtrmgr/config.boot.sample" for an example of a configuration file (note that this file MUST be modified before using it).

- Use the xorpsh command line interface after the xorp_rtrmgr is started. It should be noted that command line completion in the xorpsh does greatly simplify configuration.

A mixture of both methods is permissible. For example, a configuration file can also be loaded from within the xorpsh.

At very minimum, a router's interfaces must be configured (see Section 2.2). Typically, the FEA needs to be configured (*e.g.,* to enable unicast forwarding); the FEA configuration is described in Section 2.3. All protocol configuration is described in Section 2.4.

2.2 Network Interfaces

A XORP router will only use interfaces that it has been explicitly configured to use. Even for protocols such as BGP that are agnostic to interfaces, if the next-hop router for a routing entry is not through a configured interface the route will not be installed. For protocols that are explicitly aware of interfaces only configured interfaces will be used.

Every physical network device in the system is considered to be an "interface". Every interface can contain a number of virtual interfaces ("vif"s). In the majority of cases the interface name and vif name will be

2.4 Protocols

A unicast router typically will be configured with one or more of the following protocols: StaticRoutes (Section 2.4.1), RIP (Section 2.4.2) or BGP (Section 2.4.4).

A multicast router must have the MFEA configured (Section 2.4.5). Typically, a multicast router should have IGMP/MLD configured (Section 2.4.6). Currently, PIM-SM is the only multicast routing protocol implemented (Section 2.4.7). If some multicast-specific static routes need to be installed in the MRIB (for computing the reverse-path forwarding information), those can be specified in the StaticRoutes configuration (Section 2.4.1). If there are no unicast routing protocols configured, the FIB2MRIB module may need to be configured as well (Section 2.4.8).

2.4.1 Static Routes

This is the simplest routing protocol in XORP. It allows the installation of unicast or multicast static routes (either IPv4 or IPv6). Note that in case of multicast the routes are installed only in the user-level Multicast Routing Information Base and are used for multicast-specific reverse-path forwarding information by multicast routing protocols such as PIM-SM.

```
protocols {
  static {
    route 10.20.0.0/16 {
      nexthop: 10.10.10.20
      metric: 1
    }
    mrib-route 10.20.0.0/16 {
      nexthop: 10.10.10.30
      metric: 1
    }
    /*
    route 20:20:20:20::/64 {
      nexthop: 10:10:10:10:10:10:10:20
      metric: 1
    }
    mrib-route 20:20:20:20::/64 {
      nexthop: 10:10:10:10:10:10:10:30
      metric: 1
    }
    */
  }
}
```

identical and will map to the name given to the interface by the operating system. A virtual interface is configured with the address or addresses that should be used. At each level in the configuration hierarchy (`interface`, `vif` and `address`) it is necessary to enable this part of the configuration.

```
interfaces {
  restore-original-config-on-shutdown: false
  interface dc0 {
    description: "data interface"
    disable: false
    /* default-system-config */
    vif dc0 {
      disable: false
      address 10.10.10.10 {
        prefix-length: 24
        broadcast: 10.10.10.255
        disable: false
      }
      /*
      address 10:10:10:10:10:10:10:10 {
        prefix-length: 64
        disable: false
      }
      */
    }
  }
}
```

We recommend that you select the interfaces that you want to use on your system and configure them as above. If you are configuring an interface that is currently being used by the the system make sure that there is no mismatch in the `address`, `prefix-length` and `broadcast` arguments. If the `default-system-config` statement is used, it instructs the FEA that the interface should be configured by using the existing interface information from the underlying system. In that case, the `vif` and `address` sections must not be configured.

2.3 Forwarding Engine Abstraction

It is a requirement to explicitly enable forwarding for each protocol family.

```
fea {
  unicast-forwarding4 {
    disable: false
  }
/*
  unicast-forwarding6 {
    disable: false
  }
*/
}
```

If IPv4 forwarding is required you will require the configuration above. If the system supports IPv6 and IPv6 forwarding is required, then the `unicast-forwarding6` statement must be used to enable it [1].

[1] Note that prior to XORP Release-1.1, the `enable-unicast-forwarding4` and `enable-unicast-forwarding6` flags were used instead to enable or disable the IPv4 and IPv6 forwarding.

2.4.2 Routing Information Protocol

In order to run RIP it is sufficient to specify the set of interfaces, vifs and addresses (`interface`, `vif` and `address`) on which RIP is enabled [2].

If you wish to announce routes then it is necessary to the routes that are to be announced. For example, `connected` and `static` [3].

```
policy {
  /* Describe connected routes for redistribution */
  policy-statement connected {
    term export {
      from {
        protocol: "connected"
      }
    }
  }
}
policy {
  /* Describe static routes for redistribution */
  policy-statement static {
    term export {
      from {
        protocol: "static"
      }
    }
  }
}
protocols {
  rip {
/* Redistribute routes for connected interfaces */
/*
    export: "connected"
*/
/* Redistribute static routes */
/*
    export: "static"
*/
/* Redistribute connected and static routes */
/*
    export: "connected,static"
*/
/* Run on specified network interface addresses */
    interface dc0 {
      vif dc0 {
        address 10.10.10.10 {
          disable: false
        }
      }
    }
  }
}
```

2.4.3 Open Shortest Path First

In order to run OSPF Version 2 the `router-id` must be specified, it is a unique IPv4 address within the Autonomous System. The smallest IP address of an interface belonging to the router is a good choice.

OSPF splits networks into areas so an `area` must be configured.

Configure one or more of the routers configured interface/vif/address in this area.

The `4` in `ospf4` refers to the IPv4 address family.

```
protocols {
  ospf4 {
    router-id: 10.10.10.10

    area 0.0.0.0 {
      interface dc0 {
        vif dc0 {
          address 10.10.10.10 {
          }
        }
      }
    }
  }
}
```

2.4.4 Border Gateway Protocol

In order to run BGP the `bgp-id` (BGP Identifier) and `local-as` (Autonomous System number) must be specified.

The `peer` statement specifies a peering. The argument to the peer statement is the IP address of the peer. The `local-ip` is the IP address that TCP should use. The `as` is the Autonomous System Number of the peer.

```
protocols {
  bgp {
    bgp-id: 10.10.10.10
    local-as: 65002

    peer 10.30.30.30 {
      local-ip: 10.10.10.10
      as: 65000
      next-hop: 10.10.10.20
      /*
      local-port: 179
      peer-port: 179
      */
      /* holdtime: 120 */
      /* disable: false */

      /* IPv4 unicast is enabled by default */
      /* ipv4-unicast: true */

      /* Optionally enable other AFI/SAFI combinations */
      /* ipv4-multicast: true */
      /* ipv6-unicast: true */
      /* ipv6-multicast: true */
    }
  }
}
```

2.4.5 Multicast Forwarding Engine Abstraction

The MFEA must be configured if the XORP router is to be used for multicast routing. The MFEA for IPv4 and IPv6 are configured separately.

In the configuration we must explicitly configure the entity itself, and each `vif`. The `traceoptions` section is used to explicitly enable log information that can be used for debugging purpose [4].

```
plumbing {
  mfea4 {
    disable: false
    interface dc0 {
      vif dc0 {
        disable: false
      }
    }
    interface register_vif {
      vif register_vif {
        /* Note: this vif should be always enabled */
        disable: true
      }
    }
    traceoptions {
      flag all {
        disable: true
      }
    }
  }
}

plumbing {
  mfea6 {
    disable: true
    interface dc0 {
      vif dc0 {
        disable: true
      }
    }
    interface register_vif {
      vif register_vif {
        /* Note: this vif should be always enabled */
        disable: true
      }
    }
    traceoptions {
      flag all {
        disable: true
      }
    }
  }
}
```

Note that the interface/vif named `register_vif` is special. If PIM-SM is configured, then `register_vif` must be enabled in the MFEA.

[4] Note that prior to XORP Release-1.1, the `enable` flag was used instead of `disable` to enable or disable each part of the configuration.

2.4.6 Internet Group Management Protocol/Multicast Listener Discovery

IGMP/MLD should be configured if the XORP router is to be used for multicast routing and if we want to track multicast group membership for directly connected subnets. Typically this is the case for a multicast router, therefore it should be enabled. IGMP and MLD are configured separately: IGMP is used for tracking IPv4 multicast members; MLD is used for tracking IPv6 multicast members.

In the configuration we must explicitly configure each entity and each `vif`. The `traceoptions` section is used to explicitly enable log information that can be used for debugging purpose [5].

```
protocols {
  igmp {
    disable: false
    interface dc0 {
      vif dc0 {
        disable: false
        /* version: 2 */
        /* enable-ip-router-alert-option-check: false */
        /* query-interval: 125 */
        /* query-last-member-interval: 1 */
        /* query-response-interval: 10 */
        /* robust-count: 2 */
      }
    }
    traceoptions {
      flag all {
        disable: false
      }
    }
  }
}

protocols {
  mld {
    disable: false
    interface dc0 {
      vif dc0 {
        disable: false
        /* version: 1 */
        /* enable-ip-router-alert-option-check: false */
        /* query-interval: 125 */
        /* query-last-member-interval: 1 */
        /* query-response-interval: 10 */
        /* robust-count: 2 */
      }
    }
    traceoptions {
      flag all {
        disable: false
      }
    }
  }
}
```

A number of parameters have default values, therefore they don't have to be configured (those parameters are commented-out in the above sample configuration).

The `version` parameter is used to configure the MLD/IGMP protocol version per virtual interface [6].

[5] Note that prior to XORP Release-1.1, the `enable` flag was used instead of `disable` to enable or disable each part of the configuration.

[6] Note that the `version` statement appeared after XORP Release-1.1.

The `enable-ip-router-alert-option-check` parameter is used to enable the IP Router A option check per virtual interface [7].

The `query-interval` parameter is used to configure (per virtual interface) the interval (in secon between general queries sent by the querier [8].

The `query-last-member-interval` parameter is used to configure (per virtual interface) the m imum response time (in seconds) inserted into group-specific queries sent in response to leave group m sages. It is also the interval between group-specific query messages [9].

The `query-response-interval` parameter is used to configure (per virtual interface) the maxim response time (in seconds) inserted into the periodic general queries [10].

The `robust-count` parameter is used to configure the robustness variable count that allows tuning the expected packet loss on a subnet [11].

Note that in case of IGMP each enabled interface must have a valid IPv4 address. In case of MLD e enabled interface must have a valid link-local IPv6 address.

[7] Note that the `enable-ip-router-alert-option-check` statement appeared after XORP Release-1.1.
[8] Note that the `query-interval` statement appeared after XORP Release-1.1.
[9] Note that the `query-last-member-interval` statement appeared after XORP Release-1.1.
[10] Note that the `query-response-interval` statement appeared after XORP Release-1.1.
[11] Note that the `robust-count` statement appeared after XORP Release-1.1.

2.4.7 Protocol Independent Multicast - Sparse Mode

PIM-SM should be configured if the XORP router is to be used for multicast routing in PIM-SM domain. PIM-SM for IPv4 and IPv6 are configured separately. At minimum, the entity itself and the virtual interfaces should be enabled, and the mechanism for obtaining the Candidate-RP set (either the Bootstrap mechanism, or a static-RP set) [12].

```
protocols {
  pimsm4 {
    disable: false
    interface dc0 {
      vif dc0 {
        disable: false
        /* enable-ip-router-alert-option-check: false */
        /* dr-priority: 1 */
        /* hello-period: 30 */
        /* hello-triggered-delay: 5 */
        /* alternative-subnet 10.40.0.0/16 */
      }
    }
    interface register_vif {
      vif register_vif {
        /* Note: this vif should be always enabled */
        disable: false
      }
    }

    static-rps {
      rp 10.60.0.1 {
        group-prefix 224.0.0.0/4 {
          /* rp-priority: 192 */
          /* hash-mask-len: 30 */
        }
      }
    }

    bootstrap {
      disable: false
      cand-bsr {
        scope-zone 224.0.0.0/4 {
          /* is-scope-zone: false */
          cand-bsr-by-vif-name: "dc0"
          /* cand-bsr-by-vif-addr: 10.10.10.10 */
          /* bsr-priority: 1 */
          /* hash-mask-len: 30 */
        }
      }

      cand-rp {
        group-prefix 224.0.0.0/4 {
          /* is-scope-zone: false */
          cand-rp-by-vif-name: "dc0"
          /* cand-rp-by-vif-addr: 10.10.10.10 */
          /* rp-priority: 192 */
          /* rp-holdtime: 150 */
        }
      }
    }
```

continued overleaf....

[12] Note that prior to XORP Release-1.1, the `enable` flag was used instead of `disable` to enable or disable each part of the configuration.

```
    switch-to-spt-threshold {
      /* approx. 1K bytes/s (10Kbps) threshold */
      disable: false
      interval: 100
      bytes: 102400
    }

    traceoptions {
      flag all {
        disable: false
      }
    }
  }
}

protocols {
  pimsm6 {
    disable: false
    interface dc0 {
      vif dc0 {
        disable: false
        /* enable-ip-router-alert-option-check: false */
        /* dr-priority: 1 */
        /* hello-period: 30 */
        /* hello-triggered-delay: 5 */
        /* alternative-subnet 40:40:40:40::/64 */
      }
    }
    interface register_vif {
      vif register_vif {
        /* Note: this vif should be always enabled */
        disable: false
      }
    }

    static-rps {
      rp 50:50:50:50:50:50:50:50 {
        group-prefix ff00::/8 {
          /* rp-priority: 192 */
          /* hash-mask-len: 126 */
        }
      }
    }

    bootstrap {
      disable: false
      cand-bsr {
        scope-zone ff00::/8 {
          /* is-scope-zone: false */
          cand-bsr-by-vif-name: "dc0"
          /* cand-bsr-by-vif-addr: 10:10:10:10:10:10:10:10 */
          /* bsr-priority: 1 */
          /* hash-mask-len: 126 */
        }
      }

      cand-rp {
        group-prefix ff00::/8 {
          /* is-scope-zone: false */
          cand-rp-by-vif-name: "dc0"
          /* cand-rp-by-vif-addr: 10:10:10:10:10:10:10:10 */
          /* rp-priority: 192 */
          /* rp-holdtime: 150 */
        }
      }
    }
```

continued overleaf....

```
    switch-to-spt-threshold {
      /* approx. 1K bytes/s (10Kbps) threshold */
      disable: false
      interval: 100
      bytes: 102400
    }

    traceoptions {
      flag all {
        disable: false
      }
    }
  }
}
```

A number of parameters have default values, therefore they don't have to be configured (those parameters are commented-out in the above sample configuration).

Note that the interface/vif named `register_vif` is special. If PIM-SM is configured, then `register_vi` must be enabled.

The `enable-ip-router-alert-option-check` parameter is used to enable the IP Router Alert option check per virtual interface [13].

The `dr-priority` parameter is used to configure the Designated Router priority per virtual interface (note that in case of `register_vif` it is not used).

The `hello-period` parameter is used to configure the PIM Hello messages period (in seconds) per virtual interface [14]. It must be an integer between 1 and 18724.

The `hello-triggered-delay` parameter is used to configure the randomized triggered delay of the PIM Hello messages (in seconds) per virtual interface [15]. It must be an integer between 1 and 255.

The `alternative-subnet` statement is used to associate additional subnets with a network interface. For example, if you want to make incoming traffic with a non-local source address appear as it is coming from a local subnet, then `alternative-subnet` can be used. Typically, this is needed as a work-around solution when we use uni-directional interfaces for receiving traffic (e.g., satellite links). Note: use `alternative-subnet` with extreme care, only if you know what you are really doing!

If PIM-SM uses static RPs, those can be configured within the `static-rps` section. For each RP, an `rp` section is needed, and each section should contain the multicast prefix address the static RP is configured with. The RP priority can be modified with the `rp-priority` parameter.

If PIM-SM uses the Bootstrap mechanism to obtain the Candidate-RP set, this can be configured in the `bootstrap` section. If the XORP router is to be used as a Candidate-BSR, this should be specified in the `cand-bsr` section. For a router to be a Candidate-BSR it must advertise for each zone (scoped or non-scoped) the associated multicast prefix address. The `cand-bsr` section should contain `scope-zone` statements for each multicast prefix address. The vif name with the address that is to be used as the Candidate-BSR is specified by the `cand-bsr-by-vif-name` statement. The particular vif's address can be specified by the `cand-bsr-by-vif-addr` statement. If the `cand-bsr-by-vif-addr` statement is omitted, a domain-wide address (if exists) that belongs to that interface is chosen by the router

[13] Note that the `enable-ip-router-alert-option-check` statement appeared after XORP Release-1.1.
[14] Note that the `hello-period` statement appeared after XORP Release-1.1.
[15] Note that the `hello-triggered-delay` statement appeared after XORP Release-1.1.

itself [16]. The Candidate-BSR priority can be modified with the `bsr-priority` parameter.

If the XORP router is to be a Candidate-RP, this should be specified in the `cand-rp` section. For a router to be a Candidate-RP it must advertise for each zone (scoped or non-scoped) the associated multicast prefix address. The `cand-rp` section should contain `group-prefix` statements for each multicast prefix address. The vif name with the address that is to be used as the Candidate-RP is specified by the `cand-rp-by-vif-name` statement. The particular vif's address can be specified by the `cand-rp-by-vif-addr` statement. If the `cand-rp-by-vif-addr` statement is omitted, a domain-wide address (if exists) that belongs to that interface is chosen by the router itself [17]. The Candidate-RP priority can be modified with the `rp-priority` parameter; the Candidate-RP holdtime can be modified with the `rp-holdtime` parameter.

The `is-scope-zone` parameter is used to specify whether a Candidate-BSR `scope-zone` or a Candidate-RP `group-prefix` is scoped. Currently, scoped zones are not well tested, hence it is recommended `scope-zone` is always set to `false`. Note that typically the `hash-mask-len` should not be modified; if you don't know what `hash-mask-len` is used for, don't modify it!

The `switch-to-spt-threshold` section can be used to specify the multicast data bandwidth threshold used by the last-hop PIM-SM routers and the RPs to initiate shortest-path switch toward the multicast source. Parameter `interval` is used to specify the periodic measurement interval [18]; parameter `bytes` is used to specify the threshold in number of bytes within the measurement interval. It is recommended that the measurement interval is not too small, and should be on the order of tens of seconds.

The `traceoptions` section is used to explicitly enable log information that can be used for debugging purpose.

Note that in case of PIM-SM for IPv4 each enabled interface must have a valid IPv4 address. In case of PIM-SM for IPv6 each enabled interface must have a valid link-local and a valid domain-wide IPv6 addresses.

[16] Note that the `cand-bsr-by-vif-addr` statement appeared after XORP Release-1.1.
[17] Note that the `cand-rp-by-vif-addr` statement appeared after XORP Release-1.1.
[18] Note that prior to XORP Release-1.3, the `interval-sec` statement was used instead of `interval`.

2.4.8 FIB2MRIB

The FIB2MRIB module is used to obtain the Forwarding Information Base information from the underlying system (via the FEA), and to propagate it to the MRIB, so it can be used by multicast routing protocols such as PIM-SM. Typically, it is needed only if the unicast routing protocols (if any) on that router do not inject routes into the MRIB [19].

```
protocols {
  fib2mrib {
    disable: false
  }
}
```

[19] Note that prior to XORP Release-1.1, the `enable` flag was used instead of `disable` to enable or disable each part of the configuration.