UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERÍA
ESCUELA DE COMPUTACIÓN

"Investigación técnica de implementación e integración de Internet2"

Para optar al grado de Ingeniero en Ciencias de la Computación

Presentado por:
José Carlos Barahona Alemán

Asesor:
Ing. Cruz Antonio Galdámez

OCTUBRE DE 2006
EL SALVADOR, CENTRO AMERICA

UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERÍA
ESCUELA DE COMPUTACIÓN

Comité evaluador del trabajo de graduación:

Ing. Carlos José Tejada
Tutor

Ing. Cruz Antonio Galdámez
Asesor

Ing. Laura Yanira Salazar
Jurado

Ing. Edgardo Alberto Romero
Jurado

Ing. Evelyn Lissette Hernández
Jurado

ÍNDICE

ÍNDICE DE ANEXOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

A finales del año 1996, un grupo de 34 universidades conforman el llamado Proyecto Internet2 después de resaltar los problemas que les ocasionaba el uso del Internet actual. Internet2 es formado para proveer prioridad a las instituciones de alta educación e investigación dejando para el uso general la red comercial existente. Internet2 es el nombre que se le da al proyecto en Estados Unidos, en el resto del mundo se nombra de diferentes formas pero en general se le conoce como proyecto de Redes Avanzadas.

La misión de este proyecto es *"facilitar y coordinar el desarrollo, despliegue, funcionamiento y transferencia de tecnología de servicios y aplicaciones de red avanzados con el fin de ampliar el liderazgo de los Estados Unidos de América en el campo de la investigación y de la educación superior, y acelerar la disponibilidad de nuevos servicios y aplicaciones en Internet. Esta tarea se llevará a cabo en asociación con organismos de la Administración Federal y de los Estados (de los Estados que componen los EE.UU.) y con empresas del sector de las Tecnologías de la Computación, de las Telecomunicaciones y de la Información"*.

Un objetivo básico de las redes avanzadas es desarrollar la próxima generación de aplicaciones telemáticas para facilitar las misiones de investigación y educación de las universidades. En cada una de las que participan en el proyecto existe un equipo de desarrolladores e ingenieros que trabaja para desarrollar y hacer posibles las aplicaciones de redes avanzadas.

Las universidades de punta consideran las telecomunicaciones avanzadas como algo crítico para sus misiones de investigación y educación. Las redes avanzadas proporcionan el marco para un trabajo común en estas áreas. De forma simultánea, el proyecto hará avanzar los límites de las redes multimedia de banda ancha y ayudará a satisfacer las crecientes necesidades productivas

de las universidades miembros. Las redes avanzadas están colaborando también con empresas del sector telemático y con organizaciones sin ánimo de lucro para asegurar que los resultados se utilizan para mejorar todas las redes telemáticas, incluyendo la Internet que existe actualmente.

Las redes avanzadas proporcionan un marco para desarrollar las herramientas, las aplicaciones y las redes necesarias para conectar a las universidades miembros. Esta se basa en el desarrollo de aplicaciones de vanguardia tales como la tele inmersión, bibliotecas digitales y laboratorios virtuales. La ingeniería de redes se desarrollará cuanto sea necesario para posibilitar estas aplicaciones.

Las universidades tienen una calificación inigualable para jugar un papel protagonista en la consecución de los objetivos de las redes avanzadas porque reúnen tanto la demanda de los tipos de aplicaciones que este tipo de red desarrollará como la oferta de talento necesaria para llevar a cabo el proyecto.

En El Salvador, esta iniciativa se ve ratificada por la red RAICES (Red Avanzada de Investigación, Ciencia y Educación Salvadoreña) que cuenta entre sus miembros académicos a la Universidad Don Bosco y que en Diciembre del 2005 llevo a cabo la conexión directa con la red de RedClara (la red avanzada de la Cooperación Latino Americana de Redes Avanzadas)[1].

La presente investigación muestra un análisis de la implementación de la red avanzada en la Universidad Don Bosco al mismo tiempo que analiza la mejor forma de realizar la integración con la red y tecnología actual de la universidad.

[1] Boletín DeClara, Año1 – No 5, Diciembre 2005.

Capítulo 1

Definición del tema

1.

1.1. ANTECEDENTES

En América Latina, la iniciativa comienza en el año 2000 cuando México, por medio de su Corporación Universitaria para el Desarrollo de Internet (CUDI), se conecta a la red California Research Network (CalREN-2).

En esta iniciativa Latinoamericana se encuentra el proyecto ALICE (América Latina Interconectada Con Europa) que aglomera a varios países y sus propios proyectos de redes avanzadas. Estos proyectos se interrelacionan por medio de una red regional de telecomunicaciones llamada CLARA (Cooperación Latinoamericana de Redes Avanzadas) que cuenta entre sus miembros fundadores a la red RAICES (Red Avanzada de Investigación, Ciencia y Educación Salvadoreña) que a su vez es socio local de DANTE (Delivering

Advanced Network To Europe) para trabajar juntos en el proyecto de interconexión de América Latina con Europa por medio de las redes avanzadas.

RAICES tiene como parte de sus objetivos el desarrollo de una red de telecomunicaciones avanzada que pueda promover y coordinar el desarrollo científico, educativo y de investigación en El Salvador.

1.2. IMPORTANCIA DE LA INVESTIGACIÓN

1.2.1. Planteamiento del Problema

La red avanzada es una red de investigación que tiene como uno de sus objetivos desarrollar tecnologías nuevas que mas adelante puedan ser utilizadas por las redes de Internet comercial para el beneficio de los usuarios en general.

Por esta razón, su implementación en las redes avanzadas actualmente activas o en proceso de afiliación resulta ser un buen campo de experimentación para poder definir procedimientos que más adelante puedan ser estandarizados para su aplicación pública o privada.

Por lo anterior, las diversas variantes en los procedimientos es amplia mientras se investiga la mejor vía que represente más beneficios en su aplicación.

También, después de realizar la implementación, se llega a la etapa de integrar las actuales redes con la nueva red avanzada obteniendo el mejor resultado sin sacrificar tanto al usuario. Esto hace que la integración se convierta en objeto de un extensivo y minucioso análisis para completar satisfactoriamente la implementación.

Adicionalmente, hay que mencionar que la poca o nula información disponible bibliográficamente limita considerablemente el conocimiento del público acerca del tema, especialmente en la Universidad Don Bosco, donde se cuenta con una implementación de red avanzada con un buen grado de avance en su proceso.

1.2.2. Definición del Tema

El proyecto consiste en la investigación técnica del proceso de implementación de la red avanzada en la Universidad Don Bosco y presentar una recomendación acerca de cómo lograr una integración satisfactoria de la red actual de Internet comercial con dicha red avanzada sin causar un impacto negativo en los usuarios. Al mismo tiempo, el proyecto presentará información que cualquier usuario podrá encontrar útil para abonar a su investigación acerca del tema de redes avanzadas.

1.2.3. Justificación

Esta investigación permitirá dar a conocer información relacionada al tema de redes avanzadas que es poco difundido en el ambiente nacional y podrá estar disponible ya sea para el publico en general como para los estudiantes y docentes interesados en el tema.

El aporte principal del proyecto es proporcionar alternativas para la implementación de la red avanzada que ilustren de forma técnica el equipo a utilizar para realizar dicha implementación de la mejor forma posible, también presenta una recomendación de la integración de la red avanzada con la actual red de Internet comercial sin que el usuario pierda la actual capacidad de utilizar sus aplicaciones y al mismo tiempo aproveche las ventajas que presenta esta red.

Los beneficios que se derivan de esta investigación son los siguientes:

- Proporcionar información centralizada del tema.
- Permitir que el investigador obtenga información específica, clara y confiable acerca del tema.
- Presentar información acerca de las iniciativas, proyecciones y logros de la asociación RAICES en El Salvador.
- Apoyar cualquier asignatura relacionada con las tecnologías computacionales o de comunicación proporcionando material de apoyo o material informativo acerca del tema.
- Ilustrar técnicamente el modelo de implementación de la red avanzada.
- Realizar una recomendación sobre la implementación basándose en una comparación con el actual modelo de la Universidad Don Bosco y sus características técnicas y económicas.
- Presentar recomendaciones técnicas sobre la integración de la actual red de la Universidad Don Bosco con la nueva red avanzada.

1.3. OBJETIVOS

1.3.1. General

Presentar una investigación técnica sobre la implementación de la red avanzada y sobre su integración con la actual red de Internet comercial existente en la Universidad Don Bosco para que constituya una fuente de consulta.

1.3.2. Específicos

- Dar a conocer información acerca de la asociación de redes avanzadas en El Salvador.
- Investigar técnicamente el modelo de implementación de la red avanzada presente en la Universidad Don Bosco.
- Presentar las consideraciones necesarias para integrar la actual red de la Universidad Don Bosco con la red avanzada.
- Realizar las recomendaciones de implementación basándose en las características técnicas y factibilidad económica.

1.4. ALCANCES

El presente proyecto permitirá mostrar información acerca de las iniciativas y planes futuros sobre las redes avanzadas en el país. A continuación se detallan los alcances que se desean lograr con esta investigación:

- Investigar las iniciativas, planeaciones y logros de la asociación RAICES en El Salvador.
- Presentar las características técnicas del equipo que forme parte de los modelos de implementación.
- Analizar técnicamente la forma de integrar la actual red de la Universidad Don Bosco con la red avanzada.
- Mostrar por medio de diagramas los modelos de implementación que se investiguen.
- Se detallarán las características técnicas tales como protocolos, servicios, aplicaciones, sistemas operativos, arquitecturas y plataformas para cada recomendación de implementación.

1.5. LIMITANTES

El proyecto estará delimitado por una serie de puntos que permitirán que se desarrolle de la mejor manera. A continuación se puntualizan estas limitantes de la investigación:

- Solamente se presentarán recomendaciones derivadas del análisis técnico de la integración de ambas redes.
- Las cantidades monetarias estarán sujetas a la variación económica establecida en el momento que se presenta esta investigación.
- El estudio que se presente será teórico/técnico al igual que las recomendaciones provenientes de este.

1.6. PROYECCIÓN SOCIAL

El resultado de la investigación podrá ser utilizado por cualquier persona que presente algún tipo de interés en el tema, sean estos estudiantes, docentes o personas particulares.

Debido a la escasez de información acerca de las redes avanzadas, esta investigación ayudará a dar a conocer de qué se trata el tema y agrupara diferentes tópicos que pueden ser de utilidad para estudiantes que necesiten material de apoyo para alguna materia relacionada a las tecnologías en comunicación de redes.

La investigación complementará al análisis técnico derivado de la implementación de la red avanzada en la Universidad Don Bosco y también la ayudará como apoyo por medio de las recomendaciones que presente el proyecto acerca de la integración de su actual red de Internet comercial con la nueva red.

La investigación podrá servir como guía y referencia acerca de las iniciativas y planeaciones que tiene la asociación de redes avanzadas en El Salvador para despertar o acrecentar el interés científico y educativo de las personas sobre este tema. Este interés puede derivar más adelante en aportes e iniciativas de investigación para nuevas tecnologías que beneficien a El Salvador y ayuden a que la actual iniciativa de redes avanzadas se vuelva auto sostenible.

Capítulo 2

Investigación preliminar

2.

2.1. MARCO TEÓRICO

2.1.1. Redes Avanzadas – Definición.

Es un proyecto que agrupa un gran número de universidades y centros de investigación a nivel mundial con el objetivo principal de promover las tecnologías de redes de alta velocidad, que contribuyan al desarrollo de las aplicaciones con alta demanda de recursos tecnológicos, requeridas por el sector académico, científico y tecnológico en el ámbito de la cooperación nacional e internacional.

El eje de las redes avanzadas es un consorcio formado por aproximadamente 200 universidades de Estados Unidos con apoyo del gobierno

y algunas de las empresas líderes del sector informático y de telecomunicaciones (IBM, Intel Corporation, Cisco Systems, AT & T, Microsoft, Juniper Networks, Lucent Technologies, Qwest Communications, Sun Microsystems, por ejemplo). A este eje se le han ido incorporado universidades, organizaciones no gubernamentales relacionadas con el trabajo de redes y corporaciones interesadas en participar en el proyecto. Los usuarios finales son grupos de investigadores en diversas partes del mundo que desarrollan servicios y aplicaciones que requieren acceso a redes de alta velocidad.

Es administrada por la University Corporation for Advanced Network Development (UCAID) y, entre otras características, opera sobre una de las redes de mayor velocidad en el mundo denominada Abilene que puede alcanzar 2.4 Giga bits por segundo; recientemente fue llevada a 10 Giga bits por segundo.

Las redes avanzadas no pretenden reemplazar a la Internet actual, ni tampoco se han propuesto como principal objetivo construir una infraestructura paralela. Los participantes tienen enlaces al Internet tradicional para servicios como la Web, noticias, correo electrónico y similar. La meta del proyecto es unir a las instituciones académicas, científicas y tecnológicas nacionales y regionales con los recursos necesarios para desarrollar nuevas tecnologías y aplicaciones, que serán las utilizadas en la futura Internet.

Objetivos principales de las redes avanzadas:

- Promover el desarrollo de redes de altas prestaciones (de altas velocidades, baja latencia, con enlaces de gran capacidad, calidad de servicio, seguridad y otros) y ponerlas al servicio de la comunidad científica y de investigación.

- Facilitar el desarrollo de aplicaciones avanzadas con alta demanda de recursos.
- Asegurar la transferencia rápida de los nuevos servicios, tecnologías y aplicaciones a la comunidad Internet.

Los miembros de Internet2 (la red avanzada de Estados Unidos) crearon la red de Abilene y colaboran con frecuencia con el proyecto nacional de LambdaRail. De hecho, Internet2 y LambdaRail nacional están planeando combinarse en algún momento muy próximo, lo cual seria en algún momento entre los años 2006-2009.

La red Abilene.

Abilene es la espina dorsal de la red de alto rendimiento de los Estados Unidos y que fue creada por la comunidad de Internet2.

Más de 220 son las instituciones que participan en Abilene, sobre todo universidades con alguna corporación e instituciones afiliadas, en todos los estados de los EE.UU. así como el distrito de Columbia y de Puerto Rico.

Cuando se estableció en 1999, el Backbone de la red de Abilene tenía una capacidad de 2.5 giga bites por segundo. En 2003 una mejora a 10 giga bites por segundo comenzó y la terminación de esto fue anunciada en febrero 4 de 2004.

El nombre Abilene fue elegido debido a la semejanza de la red, en ambición y alcance, al railhead de Abilene en Abilene, Kansas, que en el 1860s representó la frontera de los Estados Unidos en el contexto de la infraestructura del ferrocarril de la nación. Una de los objetivos del proyecto es alcanzar conectividad de 100 giga bites entre cada nodo antes del fin de 2006. En armonía con la analogía railroading, el término LambdaRail se aplica a

las redes ópticas regionales que proporcionan la conectividad OC-192 en la infraestructura óptica y del paquete híbrido (HOPI, por sus siglas en ingles).

Abilene, aunque una red privada usada para la educación y la investigación, no es enteramente una red aislada, puesto que sus miembros proporcionan generalmente el acceso alternativo a muchos de sus recursos a través del Internet público. Abilene no es técnicamente parte del Internet puesto que no funciona paralelamente con las redes de Internet públicas.

LambdaRail Nacional.

Es una red nacional de alta velocidad de computadoras en los Estados Unidos que funcionan sobre líneas de fibra óptica, y es la primera red de Ethernet transcontinental. El nombre es compartido por la organización de las instituciones de investigación que desarrollaron la red, y, hasta la fecha, de los planes para continuar desarrollándola. LambdaRail es similar a la red Abilene, pero LambdaRail permite una investigación mas profunda que Abilene.

Se orienta sobre todo a los esfuerzos computacionales de ayuda del terascale, pero también no se piensa como una red de servicio, pero para ser utilizado como una plataforma de red para la experimentación con las redes de nueva generación en gran escala. LambdaRail nacional es una iniciativa basada y propietaria de las universidades, en contraste con Abilene e Internet2, que son patrocinios universidad-corporativos. Esto da a las universidades más control para utilizar la red para estos proyectos de investigación.

Los acoplamientos en la red utilizan la División de Longitud de Onda Densa que Multiplexa (DWDM, por sus siglas en ingles), que permite hasta 32 o 40 longitudes de onda ópticas individuales que se utilizarán (dependiendo de la configuración de hardware en cada extremo). Actualmente, las longitudes de onda individuales se utilizan para llevar una señal de Ethernet de 10-gigabit,

aunque otros sistemas tales como SONET se pueden también utilizar en el futuro.

Las metas del proyecto de LambdaRail Nacional son:

- Tender un puente entre la investigación de redes ópticas de última generación y la investigación de usos avanzados.
- Empujar más allá de las limitaciones técnicas y de funcionamiento de los backbones de Internet de hoy.
- Proveer al sistema cada vez mayor de proyectos de ciencia intensivamente computacionales (a menudo llamada e-Ciencia), iniciativas y experimentos de anchura de banda dedicada, características de funcionamiento determinista, y/o otras capacidades avanzadas de la red que se necesiten.
- Permitir y reencender las posibilidades de la experimentación altamente creativa, fuera de la investigación y la innovación que caracterizaron la investigación de la red con facilidad de recursos durante los años del Internet.

2.1.2. Aplicaciones de las redes avanzadas.

Las principales aplicaciones pueden ser:

- Video-conferencia de alta velocidad. La proyección de imágenes de gran resolución con sonido de alta calidad a distancia como apoyo a la educación para proporcionar material didáctico adicional a los estudiantes de colegios y universidades, características fundamentales de la educación a distancia.
- Telemedicina. La distribución de datos con garantía de calidad de servicio (QoS) y la transmisión de imágenes en alta resolución, pilares de la llamada medicina remota o telemedicina. Además, los resultados de

búsquedas en grandes bases de datos en línea permitirán al médico comparar imágenes, historiales y otras opiniones para hacer un diagnóstico altamente fiable.

- Computación en gran escala con procesos de bases de datos en múltiples sitios. Integración de diversos recursos de computación independientes, generalmente heterogéneos y distribuidos geográficamente (grids) a través de un middleware (software que traduce la información de una compañía a un formato entendible por otra empresa diferente), para brindar capacidad de cómputo y almacenamiento a gran escala, de forma transparente para el usuario.
- Ambientes de colaboración interactiva en los que se pueda intercambiar información con otros sin las barreras de las distancias (por ejemplo: investigación e instrucción interactiva basada en redes).
- Enrutamiento Multicast (Multicasting Routing): aplicaciones multimedia de gran ancho de banda. Multicast es una tecnología IP que permite a los usuarios compartir video, audio y data a través de Internet. Utiliza una suite de protocolos que hacen que los paquetes viajen a través de la red hasta múltiples receptores. Transferencia de archivos en el orden de los terabites (1024 Gbites = 240 Tbites).
- Tele inmersión, la cual permite a participantes geográficamente distantes compartir un entorno virtual que recrea su ambiente real, e interactuar en tiempo real.
- Aplicaciones que requieran comunicación a muy alta velocidad entre computadores, con garantía de calidad de servicio (Quality of Service -QoS-).
- Aplicaciones que requieran interacción hombre-computadora en tiempo real.
- Modelos en tiempo real basados en sensores.
- Acceso a recursos remotos, como telescopios o microscopios.
- Transmisión de imágenes de alta resolución.
- Laboratorios virtuales.

- Bibliotecas digitales.

2.1.3. Tecnologías derivadas de las redes avanzadas.

Entre las tecnologías que han sido desarrolladas se incluyen:

Ipv6.

Protocolo de Internet versión 6, es una capa de red estándar orientado a datos usado por los dispositivos electrónicos para comunicar datos a través de una red interna packet-switched. Después de Ipv4, es la segunda versión del Protocolo de Internet que se adoptará formalmente para uso general. Aunque había Ipv5, no era un sucesor de Ipv4; sin embargo, era un protocolo experimental, previsto para apoyar voz, vídeo y audio.

Multicast.

El multicast se utiliza a veces para referir a una difusión multiplexada.

Es la entrega de la información a un grupo de destinos simultáneamente usando la estrategia más eficiente para entregar los mensajes sobre cada vinculo de la red solamente una vez y para crear solamente copias cuando los vínculos a los destinos se dividen

Se utiliza en Ipv6 para la resolución de direcciones, y en las redes de Cero Configuración para el descubrimiento del servicio, la resolución de nombres, y la resolución de conflictos de dirección, substituyendo los protocolos de difusión ineficientes.

Calidad del Servicio (QoS, Quality of Service)

En el campo de las redes de intercambios de paquetes y del establecimiento de redes de computadoras, el término de la ingeniería del tráfico Calidad del Servicio (QoS, por sus siglas en ingles) se refiere a la probabilidad de la red de telecomunicación encontrando un contrato de tráfico dado, o en muchos casos se utiliza informalmente para referir la probabilidad de un paquete que tiene éxito en pasar entre dos puntos en la red.

2.1.4. Principales redes avanzadas.

Abilene Backbone Network

Abilene es un backbone con tecnología de avanzada que es el soporte para el desarrollo y expansión de las nuevas aplicaciones que se desarrollan dentro de la comunidad de Internet2. Abilene conecta los "network aggregation points" regionales, llamados gigaPoPs, para soportar el trabajo de las universidades miembros de Internet2, ya que ellas desarrollan aplicaciones avanzadas de Internet. Abilene complementa a otras redes de investigación de alto rendimiento.

AmericasPATH (AMPATH)

La red de AmericasPATH (AMPATH) es un proyecto de FIU (Florida International University) en colaboración con Global Crossing (GC). Utilizando la red terrestre y de fibra óptica submarina de GC, AMPATH interconectará las redes de educación e investigación en el sur y América Central, el Caribe y México a las redes de investigación y educación de los EEUU y fuera de los EEUU vía la red Abilene de Internet2.

GÉANT (Multi-Gigabit Pan-European Research Network)

GÉANT proporciona la capacidad más alta y ofrece la cobertura geográfica más grande de cualquier red de su clase en el mundo.

GÉANT es un proyecto de colaboración entre 28 redes nacionales de educación e investigación, que representan a 30 países en Europa. Su principal propósito ha sido el desarrollo de una red multi-gigabit de comunicación de datos paneuropea reservada específicamente para uso de la investigación y la educación. El proyecto también cubre otras actividades relacionadas con la investigación en el área de redes: pruebas en redes, desarrollo de nuevas tecnologías y apoyo a otros proyectos relacionados con el área de redes.

vBNS (Very High Performance Backbone Network Service)

vBNS es una red de la NSF (National Science Foundation, USA) que soporta aplicaciones de alto rendimiento y gran ancho de banda. Comenzó labores en octubre de 1994 con un acuerdo de cooperación entre MCI Worldcom y la NSF.

La red ha comenzado a operar con enlaces de 622 Mbps con la meta de llegar a utilizar 2.4 Gbps. Se espera que la red vBNS sea capaz de soportar más información y de forma más rápida que las redes de telecomunicaciones comerciales actualmente disponibles.

2.1.5. Las redes avanzadas en América Latina y El Salvador.

Proyecto ALICE (América Latina Interconectada Con Europa)

ALICE representa un significativo paso adelante hacia el desarrollo de la infraestructura de redes de investigación a través de América Latina y con Europa. Esta iniciativa aceleraría el desarrollo de la Sociedad de la Información en América Latina al proporcionar una infraestructura avanzada de

comunicación de datos que permitirá a los investigadores latinoamericanos colaborar más fácilmente en proyectos de investigación internacional avanzada. Al superar las limitaciones que existen actualmente para dicha colaboración en la región y con Europa, el objetivo perseguido es fomentar asociaciones y progreso en el campo de la investigación y la educación dentro y entre ambas regiones.

El proyecto ALICE estaría terminando en abril de 2006, tras el cual la organización CLARA, Cooperación Latinoamericana de Redes Avanzadas, garantizará la sostenibilidad de la red intraregional y la continuación de su conexión.

ALICE es coordinado por DANTE. Los socios del proyecto son:

- DANTE..... Coordinador, UK
- CLARA..... América Latina
- RETINA..... Argentina
- BolNet..... Bolivia
- RNP..... Brasil
- REUNA..... Chile
- Univ. del Cauca..... Colombia
- Crnet..... Costa Rica
- RedUniv..... Cuba
- FUNDACYT..... Ecuador
- RAICES..... El Salvador
- RAGIE..... Guatemala
- UNITEC..... Honduras
- CUDI..... México
- UNA..... Nicaragua
- RedCyT..... Panamá
- ARANDU..... Paraguay

- RAP..... Perú
- RAU..... Uruguay
- REACCIUN..... Venezuela
- RENATER..... Francia
- GARR..... Italia
- FCCN..... Portugal
- RedIRIS..... España

DANTE (Delivery of Advanced Network Technology to Europe).

DANTE planea, construye y opera las redes Pan-Europeas para la investigación y la educación. Es propiedad de European NRENs (National Research and Education Networks), y trabaja en sociedad con ellos y en cooperación con la Comisión de las Comunidades Europeas. DANTE proporciona la infraestructura de las comunicaciones de datos esencial para el éxito de los proyectos de investigación en Europa hoy.

CLARA (Cooperación Latino Americana de Redes Avanzadas).

Es una red regional de telecomunicaciones de la más alta tecnología. Interconecta a las redes académicas avanzadas nacionales de América Latina y a éstas con sus pares en Europa y el Mundo.

RAICES (Red Avanzada de Investigación, Ciencia y Educación Salvadoreña).

Es la Red Nacional de Investigación y Educación de El Salvador, es miembro fundador de CLARA (Cooperación Latinoamericana de Redes Avanzadas) y socio local de DANTE (Delivering Advanced Network To Europe) para el Proyecto ALICE (América Latina Interconecta con Europa).

Sus objetivos puntuales son los siguientes:

1. Promover y coordinar el desarrollo de redes de telecomunicaciones y cómputo, enfocadas al desarrollo científico, educativo y de investigación en El Salvador. Las actividades que se desarrollen deberán ser congruentes con los fines de las instituciones académicas que la integren y con los servicios que éstas prestan a la sociedad.
2. Promover la creación de una red de telecomunicaciones con capacidades avanzadas.
3. Fomentar y coordinar proyectos de investigación para el desarrollo de aplicaciones de tecnología avanzada de redes de telecomunicaciones y cómputo enfocadas al desarrollo científico, de la investigación y educativo de la sociedad salvadoreña.
4. Promover el desarrollo de acciones encaminadas a la formación de recursos humanos capacitados en el uso de aplicaciones educativas y de tecnología avanzada de redes de telecomunicaciones y cómputo.
5. Promover la interconexión e interoperabilidad de las redes informáticas de sus miembros.
6. Determinar las especificaciones que debe cumplir un nodo de computación con alta capacidad de transmisión digital de datos.
7. Promover el desarrollo de nuevas aplicaciones que sean de provecho para la comunidad académica y el país, y que hagan uso de la tecnología de las redes avanzadas.
8. Difundir entre sus miembros los desarrollos que realice.
9. Mantener relaciones y servir de enlace y representación ante los foros, grupos y eventos regionales y mundiales relacionados con la administración y operación de las Redes Académicas Avanzadas.
10. Administrar los fondos de la Asociación, con exclusiva atención a los fines consignados en este artículo.

11. Comprar, vender, permutar, entregar o tomar en arrendamiento o usar por cualquier otro tipo, toda clase de bienes, incluyendo muebles, inmuebles o derechos reales. En el caso de los bienes inmuebles, se estará a lo dispuesto en la Ley de Asociaciones y Fundaciones sin Fines de Lucro.
12. Solicitar, registrar, comprar, poseer en dominio, vender, permutar, explotar y otorgar los derechos a uso de patentes, solicitudes de patentes, licencias, marcas de fábrica y de comercio señales de propaganda, nombres comerciales, depósitos de obra, derechos de autor y cualquier otra forma de derecho de propiedad intelectual o industrial; así como realizar cualesquiera actividades, actos o contratos afines o conexos con la propiedad intelectual o industrial.
13. En general, emprender, ejecutar, hacer o celebrar todos los actos, operaciones convenios o contratos, necesarios, convenientes o complementarios a su funcionamiento y fines, observando las prescripciones legales sin restricción o limitación alguna.
14. Las demás que le confieren expresamente los presentes Estatutos y las necesarias para la consecución de su objeto.

Entre sus miembros académicos se encuentran las siguientes universidades:

- Universidad Centroamericana José Simeón Cañas (UCA)
- Universidad de El Salvador (UES)
- Universidad Don Bosco (UDB)
- Universidad Francisco Gavidia (UFG)
- Universidad Politécnica de El Salvador (UPES)
- Universidad Tecnológica (UTEC)
- Universidad Católica de Occidente (UNICO)
- Instituto Tecnológico Centroamericano (ITCA)

Capítulo 3

Las redes avanzadas en El Salvador

3.

La organización encargada de administrar las Redes Avanzadas en El Salvador es RAICES y se encuentra directamente relacionada a CLARA que es responsable de la implementación y manejo de una infraestructura de red que interconectará a las redes académicas nacionales (NREN) de América Latina con un gran número de universidades y centros de investigación conectados a RedCLARA.

3.1. RedCLARA

RedCLARA conecta a las redes de educación e investigación nacionales de Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, México, Nicaragua, Panamá, Perú, Uruguay y Venezuela; basada en

una topología de "anillo" con conectividad directa de 155 Mbps, RedCLARA conecta a estas redes con GÉANT a 622 Mbps.

3.1.1. Descripción Técnica

La troncal (backbone) de RedCLARA está compuesta por cinco nodos enrutadores principales, conectados en una topología de anillo. Cada nodo principal representa a un PoP para RedCLARA, y cada uno de ellos está ubicado en un país de América Latina.

Los cinco principales nodos IP de RedCLARA están ubicados en Sao Paulo (Brasil - BR), Buenos Aires (Argentina - AR), Santiago (Chile - CL), Panamá (PA) y Tijuana (México - MX). Todas las conexiones de las redes nacionales latinoamericanas (NREN) a RedCLARA serán a través de uno de estos cinco nodos. La troncal de CLARA está interconectada con la red paneuropea GÉANT a través del enlace del PoP de CLARA en Sao Paulo con el punto de acceso de GÉANT en Madrid (España - ES).

Cuando una NREN latinoamericana hace conexión con RedCLARA, lo hace a través de uno de los cinco nodos principales de la troncal de CLARA; esta conexión le brinda a estas NREN y sus miembros (clientes) acceso a RedCLARA, otorgándoles un Punto de Intercambio.

3.1.2. Configuración de los nodos principales

Circuitos SDH (Synchronous Digital Hierarchy) provistos por Global Crossing, permiten la conectividad de RedCLARA. Estos circuitos se distribuyen de la siguiente manera:

- STM-1 anillo protegido entre los Pop de RedCLARA en Buenos Aires, Sao Paulo, Santiago, Panamá y Tijuana.

- STM-4c circuito de conexión protegido, entre el PoP de RedCLARA en Sao Paulo, y el PoP de GÉANT en Madrid.

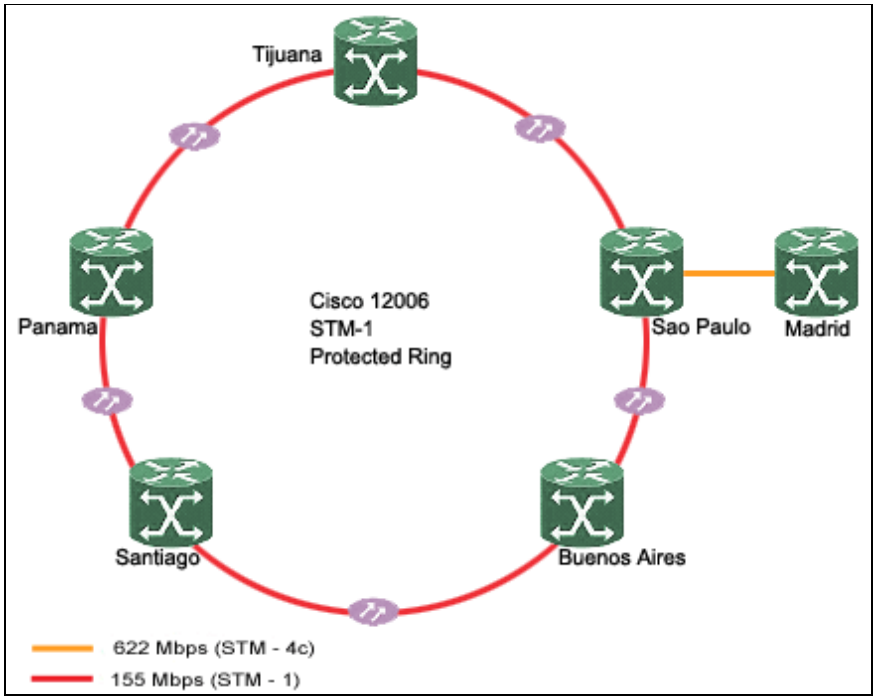


Figura 1: Diagrama de interconexión de los nodos principales de la RedClara

Cada nodo principal de RedCLARA es un Cisco 12006 Router, presentando un chasis 6-ranuras configurado con una tarjeta de línea 4-puertos OC3 POS (Packet Over Sonet) en la ranura 1, y una tarjeta de línea 4-port GE (Gigabit Ethernet) en la ranura 2. El router en Sao Paulo posee una tarjeta de línea 4-puertos OC12 POS para la conexión con Madrid, mientras que el nodo en Buenos Aires posee una tarjeta de línea 4-puertos OC3 ATM para la conexión con la NREN Argentina (RETINA).

3.1.3. PoP - configuración adicional de hardware

Para apoyar la infraestructura de PoP, se dispone de equipamiento adicional para el manejo de la configuración, desempeño y seguridad en los

nodos principales, y para recoger información de estadísticas de tráfico de los enlaces de red.

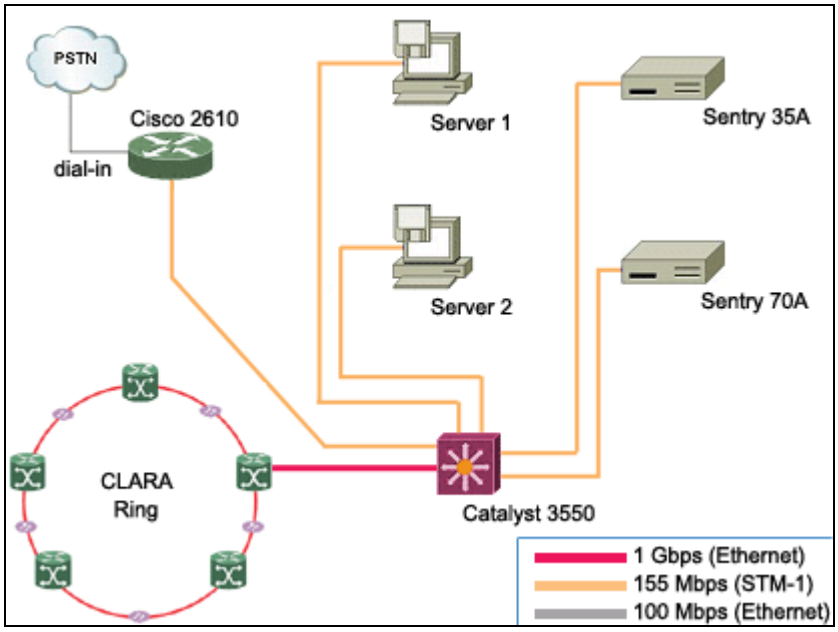


Figura 2: Diagrama de interconexión para el equipamiento de PoP de la RedClara

Cada PoP cuenta, además del router Cisco 12006, con:

- Un switch Cisco Catalyst 3550 con puertos 24 10/100 Base-TX y 2 GBIC-based puertos Gigabit Ethernet configurados con 1 GBIC SX mode.
- Un Router Ethernet Cisco 2610 One 10/100 configurado con 16 puertos Módulo Asíncrono, 1 puerto Módem Análogo y 1 puerto ISDN WAN (dial and leased line).
- Dos Servidores PC Pentium 4 - 3.4 Ghz, cada uno configurado con dos adaptadores Fast Ethernet.
- Dos módulos Sentry Remote Power Management and Distribution. El primero es de 70 Amps, para proveer alimentación de poder al Cisco 12006, y el otro es de 35 Amps y provee alimentación al resto del equipamiento.

El switch será utilizado para desarrollar una Red de Área Local (LAN) en las instalaciones de los PoP, a fin de conseguir la interconexión de los equipos para los propósitos de manejo en-banda y fuera-de-banda, y el establecimiento de la red. Los Servidores PC serán instalados con todos los programas (software) necesarios para el manejo y operación de la red por parte del Centro de Operaciones de Red (NOC) de CLARA. El router Cisco 2610 se utilizará principalmente para las operaciones de red fuera-de-banda y las mantenciones.

3.1.4. Comisión Técnica

La Comisión Técnica de CLARA es un Organismo Consultivo del Consejo Directivo de CLARA.

La Comisión Técnica está integrada por siete miembros honorarios propuestos por los Socios de CLARA; tres de ellos representan a las tres redes con mayor ancho de banda de conexión a RedCLARA, los cuatro restantes son elegidos por la Asamblea General. Esta Comisión será nombrada anualmente, pudiendo sus miembros ser renovados total o parcialmente.

El NOC (Centro de Operaciones de Red), al igual que el NEG (Grupo de Ingeniería de la Red) de CLARA, depende del Comité Técnico de CLARA, cuya propósito es el de mantener a CLARA en la frontera de los servicios avanzados de redes IP. Este objetivo debe lograrlo mediante la coordinación del NOC y el NEG. Además, el Comité Técnico debe proveer la mejor información y el más alto flujo de comunicaciones entre los grupos, protegiendo aquellos asuntos técnicos y políticos de los miembros de CLARA.

3.1.5. Operación de RedCLARA

El Centro de Operaciones de Red (NOC) de CLARA es provisto por CUDI (NREN mexicana). El NOC desempeña la operación diaria de RedCLARA. Es de responsabilidad del NOC la administración, el control, el monitoreo y la operación diaria de todas las infraestructuras físicas y lógicas que conforman la troncal de RedCLARA.

3.1.6. Ingeniería de la Red

El Grupo de Ingeniería de Red (NEG) de CLARA es provisto por RNP (NREN brasileña). El NEG desempeña el trabajo de implementación de RedCLARA y la manutención de su topología.

CLARA NEG es responsable por toda la ingeniería de red -incluida su arquitectura e implementación-, incluyendo la definición de las políticas que deberán ser adoptadas por los servicios avanzados de la troncal IP.

3.1.7. Grupos de Trabajo

Hoy los miembros de CLARA coordinan esfuerzos tendientes a llevar las distintas aplicaciones y nuevas tecnologías a las Redes Nacionales de Investigación y Educación (NREN) que la integran.

Los grupos de trabajo (GT) que se han formado con los ingenieros de las distintas NREN miembros de CLARA corresponden a las siguientes materias:

- Videoconferencia
- Voz sobre IP
- Seguridad
- Multicast
- Ipv6
- Enrutamiento Avanzado
- Mediciones

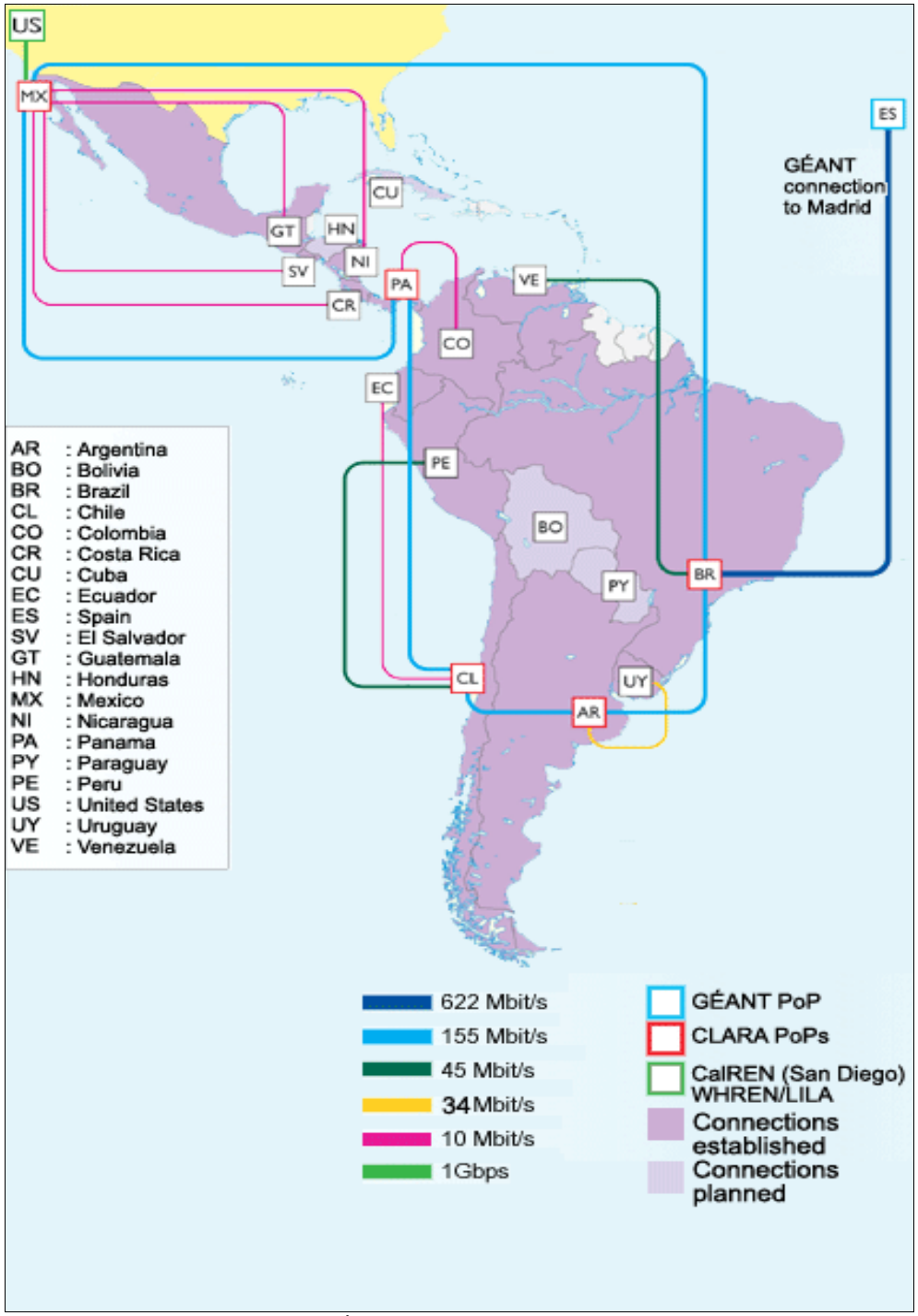
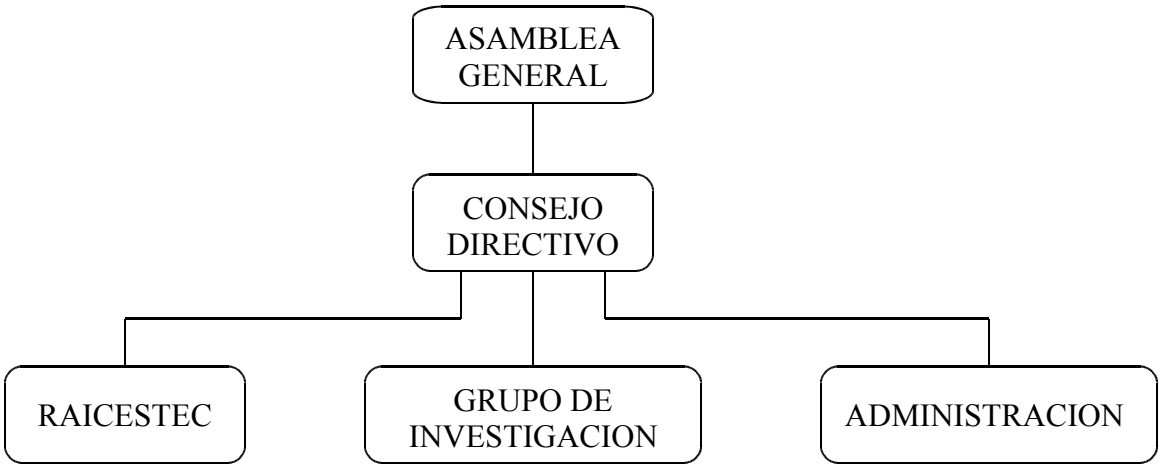


Figura 3: Topología de la Troncal de RedClara, Abril de 2006

3.2. RAÍCES

Como se mencionaba anteriormente, RAÍCES es la organización encargada de administrar las Redes Avanzadas en El Salvador. RAÍCES esta organizada de la siguiente forma:



La Asamblea General esta conformada por representantes de todas las instituciones miembros de RAÍCES.

El Consejo Directivo esta conformado actualmente de la siguiente forma:

- Presidente: Rafael Ibarra (UCA)
- Vicepresidente: Guillermo Vásquez (ITCA)
- Secretario: Carlos Newton (UFG)
- Tesorero: Carlos Bran (UDB)
- Vocales

RAICESTEC es el grupo de técnicos de RAÍCES que agrupa al Network Operation Center (NOC) y al Network Engineer Group (NEG). Actualmente el NOC y el NEG están a cargo de la Universidad Don Bosco.

Entre los logros que tiene la organización, se pueden mencionar los siguientes:

- Gestionar la donación de un Router Cisco 7206 que sirve como cabecera para conectarse a las Redes Avanzadas de CLARA. Este se encuentra actualmente ubicado en las instalaciones de Telecom.
- Haber diseñado la red local completa para el país y que se conectará con la RedClara.
- Tener el 50% de la Red Avanzada ya implementada, específicamente en la Universidad Don Bosco, Instituto Tecnológico Centroamericano, Universidad Católica de Occidente y Universidad Centroamericana José Simeón Cañas.
- Constitución del grupo técnico RAICESTEC, que se encarga del diseño, configuración y mantenimiento de la red.
- Gestión de $ 40,000 como fondos para Internetworking por medio del INSAFORP y que servirán para homogenizar los conocimientos de los técnicos de RAÍCES.
- Haber diseñado la topología y el esquema de direccionamiento de la red.

Los planes que se tiene para la organización en un futuro son los siguientes:

- Tener implementada completamente la red para el tercer trimestre del 2006.
- Que el grupo de investigación genere proyectos en conjunto con otras instituciones para el aprovechamiento de las redes avanzadas.

- Lograr la autosostenibilidad económica de la red nacional por medio de proyectos propios. Esto debido a que el financiamiento de ALICE durará hasta el año 2007.

En este momento se están trabajando en la coexistencia de la red física por medio de políticas de enrutamiento y también en las estrategias de seguridad para la red. Esta ultima tarea a cargo del NOC de RAÍCES.

La red de acceso a redes avanzadas para clientes de RAÍCES posee la estructura mostrada en la figura 4.

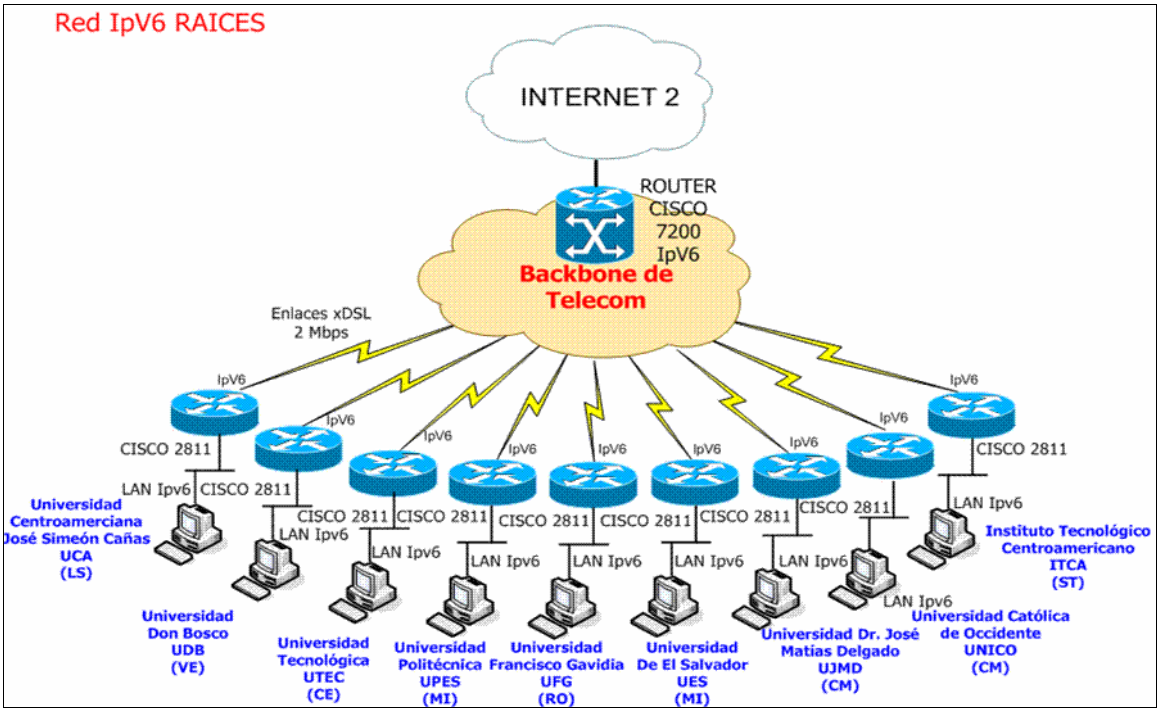


Figura 4: Esquema de conectividad de la Red RAÍCES[2]

[2] Las universidades José Matías Delgado y Politécnica actualmente se han retirado del proyecto.

Capítulo 4

Implementación de la red avanzada en la Universidad Don Bosco

4.

La Universidad Don Bosco posee actualmente una estructura de red basada en la topología de estrella extendida con ramales de backbone de fibra óptica, posee tecnología Ethernet y es completamente Full Duplex. Es esta infraestructura de red la que se esta utilizando actualmente para trabajar con las redes avanzadas.

Existen por lo menos 18 variedades de Ethernet, relacionadas con el tipo de cableado empleado y con la velocidad de transmisión (ver Anexo). En el caso de la Universidad Don Bosco se esta utilizando el tipo 100 Base-FX conocido como Fast Ethernet.

Existen dos clases de fibra óptica: monomodo (también denominado modo único); y multimodo. La fibra monomodo permite que sólo un modo de luz se propague a través de ella, mientras que la fibra multimodo permite la propagación de múltiples modos de luz. Los modos se pueden representar como haces de rayos luminosos que entran a la fibra en un ángulo determinado (ver Anexo). En la Universidad Don Bosco se utiliza la fibra multimodo.

4.1. TOPOLOGÍA DE RED DE LA UNIVERSIDAD DON BOSCO

Como ya se mencionó anteriormente, la topología de estrella extendida es la que actualmente posee la red de la Universidad Don Bosco, esto quiere decir que posee un nodo central desde el que se irradian todos los enlaces hacia los demás nodos. Por este nodo pasa toda la información que circula por la red. Luego, desde cada nodo que se conecta al nodo central surge otra red en estrella, de ahí el nombre de "extendida".

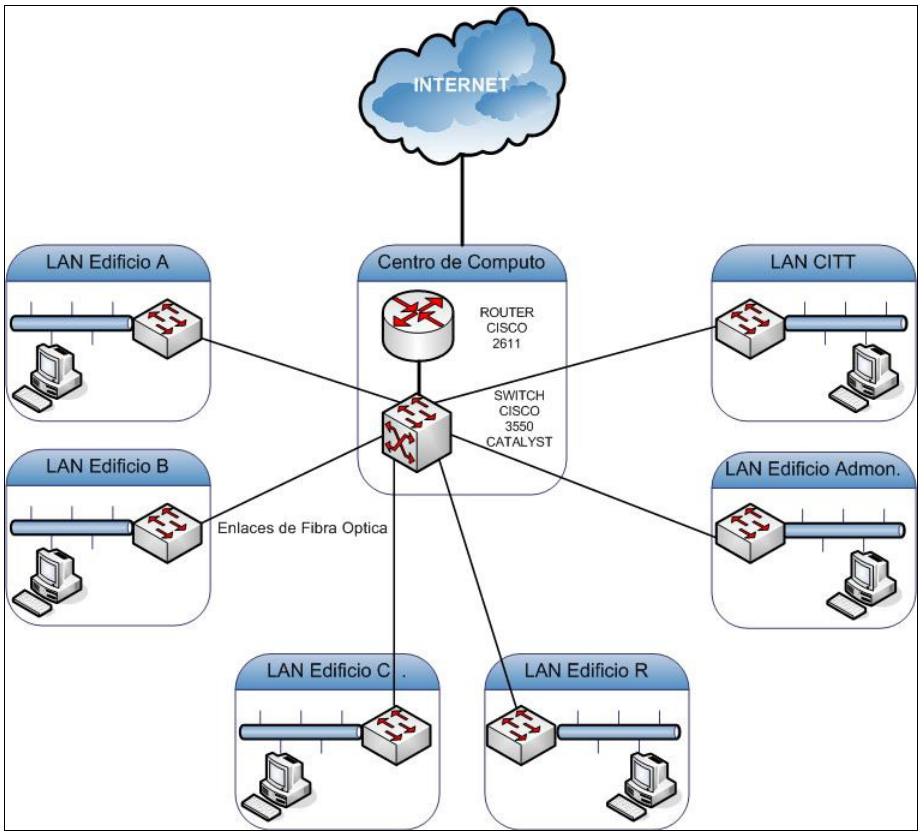


Figura 5: Red de la Universidad Don Bosco

4.2. DISPOSITIVOS DE LA RED

Dentro de la infraestructura de red de la Universidad Don Bosco se encuentran los dispositivos que conforman el núcleo central. En esta sección de la red es donde los datos se separan para dirigirse ya sea a la red de Internet o hacia las redes avanzadas, según sea el caso.

Los dispositivos que se encuentran en esta sección de la red son los siguientes:

- Router de núcleo Cisco 2611XM
- Switch de núcleo Cisco 3550 Catalyst
- Convertidores de medios para fibra óptica

Para el caso de la red avanzada se esta utilizando un Router de núcleo Cisco 2811, y por el lado del proveedor del servicio (ISP) que en este caso es la empresa Telecom, se encuentra un Router Cisco 7206 que enlaza la red avanzada del país a las demás redes de RedClara. El resto de la infraestructura es la misma que se tiene actualmente.

4.2.1. Router de Núcleo Cisco 2611XM

Figura 6: Router Cisco 2611XM

Es un Router Multiservicios que soporta Calidad de Servicio (QoS) avanzado, seguridad e integración de redes, características muy requeridas actualmente. El router Cisco 2611XM provee una ranura de modulo de red con dos puertos Ethernet 10/100 Base-T, dos ranuras integradas WIC, y una ranura para modulo de integración avanzado (AIM), con un rendimiento de hasta 20Kpps.

Especificaciones del equipo:

- 2 ranuras para tarjetas de interfase WAN (WIC).
- 1 ranura de modulo de red (NM).
- 2 puertos Fast Ethernet 10/100 Base-T.
- Un Modulo de Integración Avanzada (AIM)
- Memoria Flash de 32 MB.
- DRAM 128 MB.
- Rendimiento de 20 Kpps.

Características especiales:

- Voz y datos integrados sobre DSL: mecanismos de Calidad de Servicio avanzado mezclados con WAN de altos anchos de banda como DSL hacen posible combinar efectivamente tráficos de voz y datos en la misma conexión WAN sin sacrificar calidad o confiabilidad.
- Soporta una variedad de mecanismos de Calidad de Servicio ATM y mecanismos de Calidad de Servicio IP, proveyendo una solución escalable y administrable para transmisión de voz de alta calidad mientras se mantiene un servicio amplio de datos.
- Puede ser optimizado para redes virtuales (VPN), lo cual permite el uso seguro de cualquier red compartida incorporando las mismas políticas y niveles de seguridad.
- Incorpora tecnología Cisco IOS Firewall soportando una protección confiable y detección de intrusos.

4.2.2. Switch de núcleo Cisco 3550 Catalyst

Con una gama de configuraciones Fast Ethernet y Gigabit Ethernet, el Catalyst 3550 puede servir como un poderoso switch de capa de acceso para empresas medianas y como un switch de backbone para redes medianas.

Se pueden desplegar servicios inteligentes de ancho de banda, tales como calidad de servicio avanzado (QoS), listas de seguridad de control de acceso de Cisco, administración multicast y ruteo IP de alto rendimiento.

Figura 7: Switch Cisco 3550 Catalyst

Especificaciones del equipo:

- 24 puertos Ethernet 100 base-FX.
- 2 puertos Gigabit Ethernet 1000 base-X.
- 1 puerto de consola.
- Dispositivo de poder interno AC 100/240 V (50/60 Hz).
- 1 conector RPS externo para fuente redundante externa.
- RAM 64 MB.
- Memoria Flash 16 MB.
- Rango de transferencia de datos de 100 Mbps.

Características especiales:

- Protocolos de conexión de datos Ethernet y Fast Ethernet.
- Protocolos de administración remota SNMPv1, SNMPv2c, SNMPv3, RMON I y II estándar.
- Características:
    - Capacidad Full Duplex.
    - Auto sensibilidad por dispositivo.
    - Ruteo IP.
    - Soporte DHCP.
    - Auto negociación.
    - Soporte VLAN.
- Compatible con los siguientes estándares:

  - IEEE 802.1x
  - IEEE 802.1w
  - IEEE 802.1s
  - IEEE 802.3x full duplex en puertos 10BASE-T, 100BASE-TX, y 1000BASE-T
  - IEEE 802.1D Spanning-Tree Protocol
  - IEEE 802.1p CoS Prioritization
  - IEEE 802.1Q VLAN
  - IEEE 802.3ad
  - IEEE 802.3 10BASE-T
  - IEEE 802.3u 100BASE-TX
  - IEEE 802.3ab 1000BASE-T
  - IEEE 802.3z 1000BASE-X
  - 1000BASE-X (GBIC)
  - 1000BASE-SX
  - 1000BASE-LX/LH
  - 1000BASE-ZX
  - 1000BASE-CWDM GBIC 1470nm
  - 1000BASE-CWDM GBIC 1490nm
  - 1000BASE-CWDM GBIC 1510nm
  - 1000BASE-CWDM GBIC 1530nm
  - 1000BASE-CWDM GBIC 1550nm
  - 1000BASE-CWDM GBIC 1570nm
  - 1000BASE-CWDM GBIC 1590nm
  - 1000BASE-CWDM GBIC 1610nm
- Seguridad dinámica basada en el puerto para prevenir que clientes sin autorización tengan acceso a la red.

- Características integradas al Cisco IOS para optimización del ancho de banda.
- Incluye el Standard Multilayer Software Image (SMI) o el Enhanced Multilayer Software Image (EMI). El SMI incluye QoS avanzado, limite de rangos, listas de control de acceso (ACL's) y protocolo de información de rutas (RIP). El EMI provee un set más rico de características empresariales incluyendo ruteo IP unicast y multicast avanzado basado en hardware y el protocolo de comunicación Web Cache (WCCP).

4.2.3. Convertidor de Medios para fibra óptica

En la estructura de red de la Universidad Don Bosco, se utilizan convertidores de medios 100 Base-Tx a 100 Base-Fx con conectores ST. Estos convertidores son marca Allied Telesyn MC101XL.

Figura 8: Convertidor Allied Telesyn MC101XL

Estos convertidores Fast Ethernet permiten extender el tamaño de redes UTP y de fibra multimodales usando el cable de fibra. Pueden ser usados para extender la línea en hasta 2,000m. Conectando los convertidores con conmutadores Fast Ethernet conectan automáticamente los eslabones en ambos Full o Half-Duplex, favoreciendo el establecimiento del ancho de banda. Estos convertidores con UTP poseen el switch interno MDI/MDIX, que permite al convertidor conectarse con PC, concentrador o conmutador con el cable simple UTP. Además, permiten comprobar la integridad de la conexión.

Tiene las siguientes características:

Tabla 1: Características del convertidor de medios Allied Telesyn MC101XL

Tecnología de conectividad	Cableado
Tipo de cableado	100 Base-Fx, 100 Base Tx
Protocolo de interconexión de datos	Fast Ethernet

Velocidad de transferencia de datos	100 Mbps
Distancia máx. De transferencia	2,000 mts.
Características	Half Duplex, Full Duplex
Característica de intercambio	Auto MDI/MDIX
Cumplimiento de norma	802.3U, transparente para paquetes 802.1Q
Interfaces	1 x red – Ethernet 100 Base-Fx – modo múltiple ST hembra – 2
Conexiones	1 x red – Ethernet 100 Base-Tx – RJ-45 macho – 1
Dispositivo de alimentación	Adaptador de corriente – Externo
Voltaje necesario	CA 110/220 V ± 10% (50/60 Hz)

4.2.4. Router de Núcleo Cisco 2811

Es un Router de Servicios Integrados que esta optimizado para dar servicios de seguridad, envío de datos concurrentes a alta velocidad, voz y video.

Figura 9: Router Cisco 2811

Especificaciones del equipo:

- 4 Slots para Tarjetas de Interfase de alta velocidad HWIC.
- 1 Slot de Compact Flash (64 – 256 MB).
- 2 puertos USB para dispositivos Cisco futuros aprobados.
- 1 puerto de consola.
- 1 puerto auxiliar.
- 1 conector RPS externo para fuente redundante externa.
- 1 slot de modulo de red NME.
- Fuente AC, 2A (110 V) 1A (230 V).
- 2 puertos Fast Ethernet 10/100 base T.
- DRAM 256 – 768 MB.

Características especiales:

- El Cisco 2811 es un router de servicios integrados (voz, datos y video), el cual agrega procesamientos de seguridad, memoria y servicios concurrentes. Puede ser utilizado para negocios pequeños, medianos y proveedores de servicios.
- Funcionamiento wire-speed (alta velocidad) para servicios concurrentes como seguridad, voz y video, y servicios avanzados para múltiples T1/E1/xDSL WAN rates.
- Protección de la inversión a través de funcionamiento y modularidad crecientes.
- Soporte para mas de 90 módulos de red y para la mayoría de AIM's, NM's, WIC's, VWIC's y VIC's existentes.
- Soporte opcional para conmutación de capa 2, con Power over Ethernet (PoE).
- Provee diversos servicios de seguridad como:
    - Encriptación on-board.
    - Soporte para mas de 1500 VPN túneles con el modulo AIM-EPII-PLUS.
    - Soporte de defensa con antivirus a través del Network Admisión Control (NAC).
    - Soporte para prevención de intrusos, así como soporte stateful Cisco IOS Firewall y otras características esenciales de seguridad.
    - Soporta Aceleración de encriptado VPN IPSec Digital Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES) 128, AES 192 y AES 256 sin consumir ninguna ranura AIM.
- Cobertura para tecnología LAN inalámbrica, proveyendo capacidades de costo-efectividad, seguridad inalámbrica.
- Provee servicios integrados de voz, telefonía básica, procesamiento de llamadas, mensajería y servicios automatizados.

- Soporte para Cisco IOS software release 12.3T.

4.2.5. Router de RAICES en el ISP, Cisco 7206

El Router de Servicios Agregados, Cisco 7206, tiene seis ranuras para puertos horizontales y provee hasta 2 Mbps de rendimiento en ruteo e incluye función habilidad para intercambio de multiservicios integrados (MIX).

Figura 10: Router Cisco 7206

Con velocidades de procesamiento de hasta 2 millones de paquetes por segundo, rangos de servicios y puertos desde NxDS0 hasta Gigabit Ethernet, y OC-3 así como un sinnúmero de servicios IP, el Cisco 7206 VXR es ideal para Servicios Agregados WAN/MAN para empresas y proveedores de servicio (ISP) desplegando cualquiera de las siguientes soluciones:

- Funcionamiento de la característica Quality-of-Service (QoS) para WAN
- Ancho de banda agregada hasta 16,000 sesiones Point-to-Point Protocol (PPP) por equipo.
- Multiprotocol Label Switching Provider Edge (MPLS PE), selección numero uno para el despliegue de los proveedores actuales.
- Integración voz/video/dato, multiplexor de división de tiempo (TDM) activado con adaptadores de puerto de voz.
- Soporte IP-to-IP Gateway e interconexiones IP directas.
- Seguridad IP para redes virtuales privadas (IPSec VPN), escalable a 5,000 túneles por equipo.

A través de la integración de funciones previamente desarrolladas por separado en una misma plataforma, el Cisco 7206 VXR provee una plataforma que soporta:

- Interfaces LAN y WAN de alta densidad.

- Agregado de servicios de ancho de banda, incluyendo PPP, terminación RFC 1483 y túneles Layer 2 Tunneling Protocol (L2TP).
- Terminaciones de entronque digital T1/E1 para voz, video y datos.
- Multicanales de alta densidad T3/E3 y T1/E1 con unidad de servicio de canal/unidad de servicio de datos integrado (CSU/DSU).
- Conectividad ATM, Packet over SONET (POS) y Dynamic Packet Transport (DPT).
- ATM IMA (Inverse Multiplexing over ATM) para voz, video y datos.
- Conectividad directa al canal IBM Mainframe.
- Light-density Layer 2 Ethernet switching.

Características del equipo:

- 6 Ranuras configurables sin Port Adapter Jacket Card.
- 7 Ranuras configurables con Port Adapter Jacket Card.
- 48 Puertos Ethernet (10 BASE-T).
- 30 Puertos Ethernet (10 BASE-FL).
- Hasta 6 Puertos Fast Ethernet (TX).
- Hasta 6 Puertos Fast Ethernet (FX).
- 2 Adaptadores de Puerto EtherSwitch.
- Hasta 6 Puertos 100VG-AnyLAN.
- Hasta 6, 4 Puertos ATM (T3, OC-3).
- 6 Packets over SONET.
- 1 Adaptador de puerto ATM-CES (Data, Voice, Video), Dual-Wide.
- 24 Puertos Token Ring (FDX, HDX).
- 48 Puertos Seriales Síncronos.
- 24, 48 Puertos ISDN BRI (U, S/T).
- 48 Puertos ISDN PRI, Multicanal T1/E1.
- Hasta 6 Puertos multicanal T3.
- Hasta 12 Puertos HSSI.

- Hasta 14 Puertos Packet over T3/E3 (Integrated DSU).
- 6 Puertos de interfase Canal IBM (ESCON and Parallel).
- 1 Modulo de aceleración VPN.
- 128 MB – 1 GB de memoria para el procesador.
- 48 – 128 MB, 64 – 256 MB de capacidad para tarjeta de memoria flash PCMCIA (hasta 2 ranuras disponibles).
- 64 – 256 MB de capacidad para tarjeta de memoria Compact Flash.

Características especiales:

- Trae una ranura para un controlador de entrada/salida (I/O). Los siguientes tipos de controladores son soportados:
  - C7200 VXR-I/O, Controlador I/O Cisco 7200 VXR
  - C7200 VXR-I/O-2FE/E, Controlador I/O Cisco 7200 VXR con auto sensibilidad dual para puertos Ethernet 10/100.
  - C7200 VXR-I/O-GE+E, Controlador I/O Cisco 7200 VXR con un puerto convertidor de interfase Gigabit Ethernet (GBIC) y un puerto Ethernet.
- Ofrece una densa escalabilidad con el rango más amplio de opciones de conectividad, incluyendo:
  - Ethernet 10BASE-T y 10BASE-FL.
  - Fast Ethernet 100 BASE-T (RJ-45 y MII).
  - Gigabit Ethernet.
  - Token Ring (half y full duplex).
  - Serial Síncrono ISDN BRI, PRI, HSSI, T3, E3.
  - Multicanal T1, ISDN PRI.
  - Multicanal E1, ISDN PRI.
  - Multicanal T3, E3.
  - Multicanal STM-1.

  - Packet over SONET (POS).
  - Dynamic Packet Transport (DPT).
  - ATM (modo simple y multimodo).
  - ATM-CES.
  - Digital Voice Port Adapter, Enhanced.
  - Mix-enabled T1/E1.
  - Integrated Service Adapter (ISA).
  - VPN Acceleration Module (VAM).
  - VPN Service Adapter (VSA).
- Otras características soportadas por el Cisco 7206 VXR:
  - Cisco Express Forwarding.
  - QoS.
    - Low-Latency Queuing (LLQ).
    - Class-Based Weighted Fair Queuing (CBWFQ).
    - Class-Based Weighted Random Early Detection (CBWRED).
    - Policing.
    - Marking.
    - Shaping.
    - Committed Access Rate (CAR).
    - Generic Traffic Shaping (GTS).
    - Frame Relay Traffic Shaping (FRTS).
    - Soporte para interfase Modular QoS command-line (MQC).
    - Network-Based Application Recognition.
  - MPLS.
    - MPLS VPN.
    - MPLS QoS.
    - Ingeniería de tráfico MPLS.

        - Cualquier transporte sobre MPLS.
    - Agregado de ancho de banda.
        - PPPoX.
        - RBE.
        - PPP over X (PPPoX) con L2TP.
        - MLPPP.
    - Multiservicio/voz.
        - cRTP.
        - LFI.
        - FRF11/12.
        - MLPPP.
        - MLFR.
        - IP-to-IP Voice Gateway.
        - SRST.
    - Tunneling.
        - GRE.
        - L2TP.
        - UTI.
        - L2TPv3.
        - 6to4.
    - Otros.
        - ACLs.
        - NAT.
        - Net Flow.
        - Firewall.
        - Multicast.
        - Flexible Packet Matching.

- IPSec VPN.
- Secure Multicast.
- IPv6.

- Entre los protocolos estándar de Internet que soporta se pueden mencionar los siguientes:
  - Protocolos Layer 2 y Layer 3-Address Resolution Protocol (ARP), IPCP, IP forwarding, IP host, IP Multicast, PPP-over-ATM, TCP, Telnet, Trivial File Transfer Protocol (TFTP), User Datagram Protocol (UDP), transparent bridging, virtual LAN (VLAN), MPLS, e IPv6.
  - Protocolos de ruteo Layer 3-EIGRP, IGRP, IS-IS, OSPF, BGP, PIM, y RIP.
  - Administración de red y seguridad-AAA, CHAP, FTP, RADIUS, SNMP, PAP, y TACACS.
  - RFC 1483 - Encapsulamiento multiprotocolo sobre ATM AAL 5.
  - RFC 1577-IP clásico y ARP sobre ATM AAL 5.
  - IP or IP over ATM.
  - Serial Line Internet Protocol (SLIP).
  - Dynamic Host Connection Protocol (DHCP).
  - Hot Stand by Router Protocol (HSRP).

4.3. INFRAESTRUCTURA DE LA RED AVANZADA EN LA UNIVERSIDAD DON BOSCO

El esquema de conectividad de la red avanzada en la Universidad Don Bosco es similar al que se muestra en la figura 11.

Como se observa en dicho diagrama, la red avanzada está funcionando dentro de la actual infraestructura de red, la misma LAN en la que esta configurado el acceso a la red Internet.

Para lograr la coexistencia de ambas redes dentro de la misma infraestructura se utilizan técnicas de políticas de enrutamiento en el switch de núcleo. También se esta utilizando el protocolo Ipv4 para ambas redes.

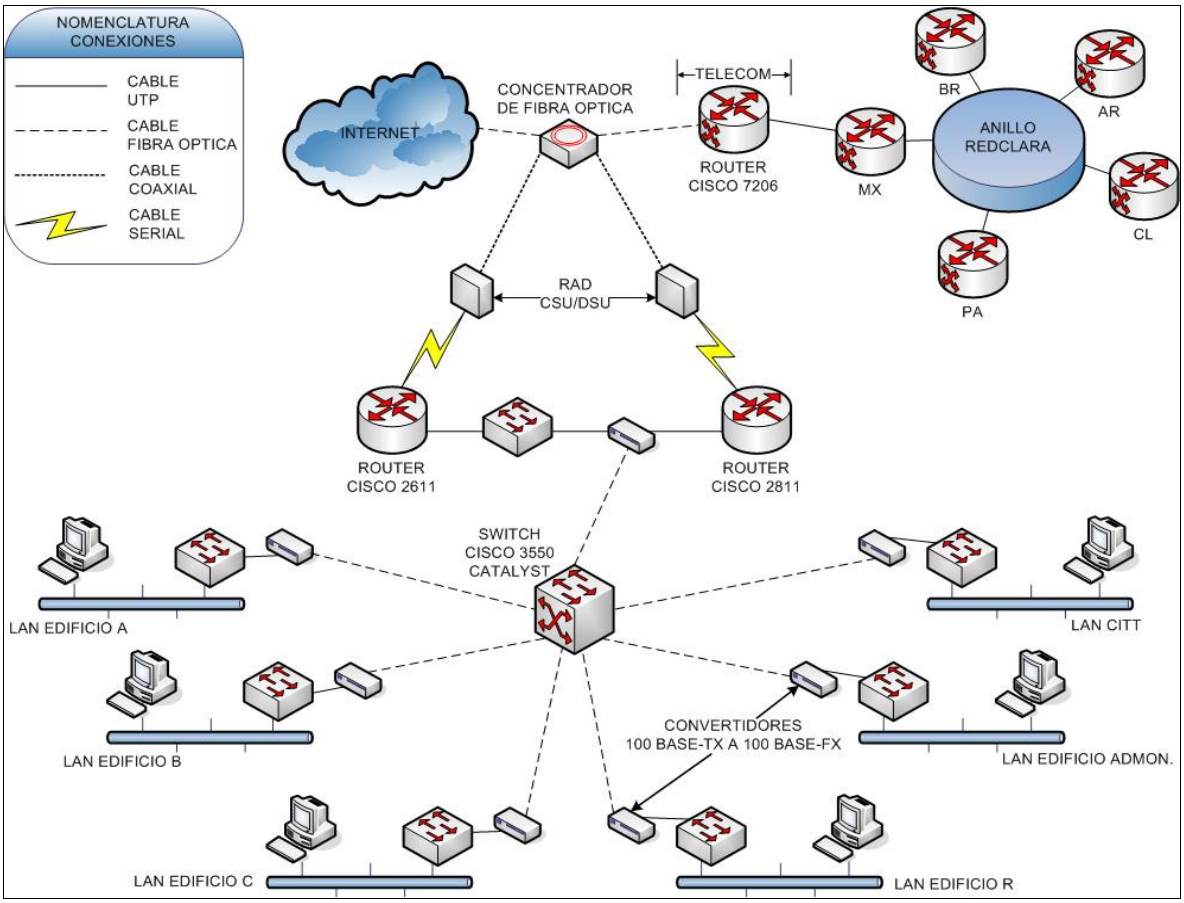


Figura 11: Esquema de conectividad de la Universidad Don Bosco

Los datos que se transmiten desde la red avanzada de la Universidad Don Bosco, luego de alcanzar al Router del ISP que en este caso es el Cisco 7206, pasan a un nodo principal del anillo de la RedClara y de ahí se distribuyen hacia las demás redes avanzadas hasta alcanzar su destino final. El nodo al que se encuentra conectada la Red Avanzada de El Salvador esta ubicado en México.

4.4. PROPUESTAS EN LA IMPLEMENTACIÓN DE LA RED AVANZADA PARA LA UNIVERSIDAD DON BOSCO

La actual red de la Universidad Don Bosco está configurada usando la topología de estrella extendida y además incluye otras características que la convierten en un eficiente medio de transmisión de datos dentro de la institución.

Una de estas características es que utiliza Fibra Óptica en el núcleo central; esto permite proporcionar un backbone de alta velocidad a todas las demás subredes que dependen de dicho núcleo.

También, por el hecho de utilizar la configuración "extendida" de la topología de estrella, permite limitar la cantidad de dispositivos que se deben interconectar al nodo central y al mismo tiempo el cableado se reduce considerablemente.

Pero las características que convierten a esta red en un modelo eficiente y fácil de mantener es que permite la flexibilidad al momento de incrementar el número de maquinas conectadas a la red, si alguna de las computadoras falla la red no se ve afectada en su funcionamiento y el diagnostico de problemas se vuelve simple y rápido.

Debido a todo lo anterior, las alternativas de implementación de la red avanzada se reducen a recomendaciones en el equipo que se pueda utilizar para ponerla a funcionar.

4.4.1. Propuesta para el Switch de Núcleo

Como alternativas al Switch de núcleo Cisco 3550 Catalyst se propone el siguiente equipo:

- Switch Cisco 3750 Catalyst

- Switch 3Com 5500 – EI

4.4.1.1. Switch Cisco 3750 Catalyst

Figura 12: Switch Cisco 3750 Catalyst

El Cisco 3750 Catalyst facilita el despliegue de aplicaciones y se adapta a las necesidades cambiantes de la organización proveyendo flexibilidad de configuración y automatización de configuraciones de redes y servicios inteligentes. Además está optimizado para despliegues de Gigabit Ethernet de alta densidad. El Cisco 3750 Catalyst esta disponible con el IP Service Image que incluye Calidad de Servicio (QoS) Avanzado, Listas de Control de Acceso (ACLs), Protocolo de Información de Ruteo (RIP) y ruteo IP Unicast y Multicast avanzado basado en hardware.

Características del equipo:

- 24 puertos 100 Base-FX.
- 2 puertos SFP Gigabit Ethernet.
- 1 puerto serial de administración.
- 32 Gbps stacking bus de alta velocidad.
- 128 MB Memoria RAM.
- 32 MB Memoria Flash.
- Rango de transferencia de datos de 100 Mbps.
- Protocolo Data Link Fast Ethernet.

Características especiales:

- Smart Multicast aumentando la eficiencia de aplicaciones multicast, como video.
- Calidad de Servicio (QoS) superior manteniendo el flujo de datos aún a velocidades de Gigabit Ethernet.
- Seguridad de la red incluyendo ACLs, autenticación, seguridad a nivel de puerto, servicios de identificación de redes con 802.1x y sus extensiones.
- Administración de IP Simple para actividades como detección de errores, creación y modificación de VLANs, seguridad de red y controles de QoS.
- Soporte Ipv6 con capacidad para ruteo por hardware para máximo desempeño.
- Soporta Protocol Independent Multicast (PIM) para ruteo IP Multicast, incluyendo PIM Sparse Mode (PIM-SM), PIM Dense Mode (PIM-DM) y PIM Sparse-Dense Mode.

4.4.1.2. Switch 3Com 5500 – EI

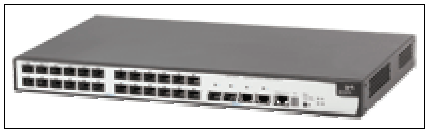


Figura 13: Switch 3Com 5500 - EI

El 3Com 5500 es un switch Fast Ethernet basado en fibra que soporta ruteo avanzado en Layer 3 y QoS en Layer 2 – 4. Posee el software Enhanced Image (EI) para ejecutar las aplicaciones de red más demandantes. Posee 24 puertos SFP, dos puertos Gigabit y dos puertos 10/100/1000 disponibles para stacking, conexiones entre switches y up links a la red. El 3Com 5500 provee extensas características de seguridad como SNMP v3, SSH y logeo de red.

Características del equipo:

- 24 puertos 100 Base-X
- 2 puertos Gigabit SFP
- 2 puertos de auto negociación 10 Base-T/100 Base-TX/1000 Base-T

- 1 Puerto de poder RPS (-48 VDC)
- 1 Puerto para consola
- 26 ranuras de expansión libres
- Control de flujo Full Duplex 802.3x
- Fuente de poder interna 50/60 Hz AC, 90 – 240 VAC

Características especiales:

- Combinable hasta con 8 unidades más o 384 puertos Fast Ethernet usando 2 Gbps de ancho de banda (4 Gbps Full Duplex).
- 12.8 Gbps de capacidad de switching.
- Operación multicapa con ruteo estático, función habilidad Layer 3 basado en RIP, OSPF, PIM – SM y PIM – DM.
- Avanzado ACLs para restricción de accesos no autorizados y corrupción de datos.
- Autenticación por usuario y encriptación DES 56-BIT o 168-BIT para asegurar protocolos Layer 3.
- IEEE 802.1p Class of Service/Quality of Service (CoS/QoS).
- Clasificación, priorización y filtrado Ipv6.

4.4.1.3. Análisis Comparativo

A continuación se muestra un cuadro comparativo de las características[3] del equipo que actualmente se esta utilizando con las del equipo propuesto.

Tabla 2: Análisis técnico comparativo de switches propuestos

	Cisco 3550 Catalyst	Cisco 3750 Catalyst	3Com 5500 – EI
Memoria RAM	64 MB	128 MB	n/a
Memoria Flash	16 MB	32 MB	n/a
Puertos	24	24	28
Rango de Transferencia de	100 Mbps	100 Mbps	100 Mbps

[3] Características basadas en configuración de fábrica.

Datos			
Protocolo Data Link	Fast Ethernet	Fast Ethernet	Fast Ethernet
Protocolo de ruteo	Requiere el software Enhanced Multilayer Image (EMI)	OSPF, IGRP, BGP-4, RIP-1, RIP-2, EIGRP, HSRP, DVMRP, PIM-SM, ruteo estático IP, PIM-DM	OSPF, RIP-1, RIP-2, IGMPv2, IGMP, PIM-SM, PIM-DM
Protocolo de Administración Remota	SNMP 1, SNMP 2, RMON 1, RMON 2, Telnet	SNMP 1, SNMP 2, RMON, Telnet, SNMP 3, http	RMON 1, SNMP, Telnet, SNMP 3, HTTP
Tecnología de Conectividad	Cableado	Cableado	Cableado
Modo de Comunicación	Half-duplex, full-duplex	Half-duplex, full-duplex	Half-duplex, full-duplex
Protocolo de intercambio	Ethernet	Ethernet	Ethernet
Tamaño tabla direcciones MAC	8K	12K	16K
Características	Capacidad Full duplex, ruteo, layer 3 switching, layer 2 switching, ruteo IP, soporte VLAN, administrable	Capacidad Full duplex, ruteo, soporte DHCP, auto-negociación, soporte ARP, trunking, balance de carga, soporte VLAN, IGMP snooping, combinable, soporte Ipv6	Control de flujo, layer 3 switching, soporte DHCP, auto-negociación, soporte VLAN, IGMP snooping, combinable, 3Com XRN Technology, soporte Ipv6
Estándares compatibles	IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.3x, IEEE 802.1w, IEEE 802.1x, IEEE 802.1s	IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.3af, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s	IEEE 802.3, IEEE 802.3U, IEEE 802.3i, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.3ae, IEEE 802.1s
Ranuras de expansión libres	2 x GBIC	2 x SFP (mini-GBIC)	26 x SFP (mini-GBIC)
Interfase	24 x red - Ethernet 100Base-FX 1 x administración - RJ-45	24 x red - Ethernet 100Base-FX - MT-RJ multi-modo 1 x administración - consola - RJ-45 2 x NSD	2 x red - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45 1 x administración - consola - RJ-45
MTBF	186,000 horas	269,011 horas	184,000 horas
Algoritmo de encriptación	n/a	n/a	MD5
Método de autenticación	Kerberos, Secure Shell (SSH), RADIUS, TACACS+	Kerberos, Secure Shell (SSH), RADIUS, TACACS+	Secure Shell (SSH), RADIUS
Dispositivo de poder	Fuente interna	Fuente interna	Fuente interna
Voltaje requerido	AC 120/230 V (50/60	AC 120/230 V (50/60	AC 120/230 V (50/60

	Hz)	Hz)	Hz)
Garantía	De por vida	De por vida	De por vida
Temperatura de operación mínima	32 F	32 F	32 F
Temperatura de operación máxima	113 F	113 F	104 F
Rango de humedad operacional	10 - 85%	10 - 85%	10 - 95%
Rango de Precio	$ 3,735.99 – 4,819.99	$ 6,908.00 – 8,039.99	$ 1,895.00 – 2,430.00

Como se observa en la tabla 2, tanto el Cisco 3750 Catalyst como el 3Com 5500 – EI mejoran la mayoría de características del Cisco 3550 Catalyst y en algunos casos las aumentan, como sucede con los protocolos de ruteo y los estándares soportados. También se observa que el 3Com 5500 - EI introduce el algoritmo de encriptación MD5 como una mejora comparado a los otros dos equipos.

Ambos equipos propuestos poseen las características necesarias para poder sustituir al actual equipo utilizado en la red mejorándolas o aumentándolas. Estos equipos propuestos soportan los protocolos de ruteo PIM – SM y PIM – DM que serían necesarios en el caso de querer implementar Multicast en la red avanzada. También soportan el protocolo Ipv6 para su futura implementación.

Las ventajas que proporciona el Cisco 3750 son las siguientes:

- Mayor memoria RAM y Flash.
- Capacidad de soportar una serie de protocolos de ruteo, entre los que se incluyen el PIM – DM y el PIM – SM que son utilizados en la implementación de Multicast.
- Incluye mejoras de función habilidad como el 802.3af Power over Ethernet (PoE), mayor densidad en la Gigabit Ethernet y ruteo Ipv6 por hardware.
- Proporciona mayor seguridad por medio de Inspección Dinámica ARP, IP Source Guard y DHCP Snooping.

Entre las desventajas se tienen:

- Disminuyen los ruteos Unicast de 16000 a 11000.
- Mayor costo por unidad.

Las ventajas que proporciona el 3Com 5500 – EI son las siguientes:

- Similares características a las que posee el switch Cisco 3750.
- Capacidad para soportar los protocolos de ruteo PIM – DM y PIM – SM.
- Menor costo que el otro equipo recomendado.

Entre las desventajas que tiene este equipo se encuentran:

- No posee el protocolo CGMP (Cisco Group Management Protocol) que le permite a un switch funcionar como un Cisco Group Management Protocol router para otros switches cliente.
- Requiere convertidor para compatibilidad con fibra multimodo 100 Base-FX.

4.4.1.4. Recomendación técnico financiera

En base al análisis comparativo, el equipo que mejora notablemente las características del Cisco 3550 es el Cisco 3750. También mejora los servicios que se prestan en la red y previene la implementación de las nuevas tecnologías como QoS, multicast e Ipv6.

Por esto, el equipo que se recomienda en base a sus ventajas técnicas es el Cisco 3750 Catalyst.

Tabla 3: Análisis financiero de la depreciación del Cisco 3550

Años de uso	Valor a depreciar (precio original)	Depreciación	Saldo a depreciar (precio actual)	Depreciación acumulada
1	$ 4,819.99	$ 963.99	$ 3,855.99	$ 963.99
2	$ 4,819.99	$ 963.99	$ 2,892.00	$ 1,927.99
3	$ 4,819.99	$ 963.99	$ 1,928.00	$ 2,891.99
4	$ 4,819.99	$ 963.99	$ 964.00	$ 3,855.99

5	$ 4,819.99	$ 963.99	$ 0.00	$ 4,819.99

La tabla 3 muestra el análisis financiero de la depreciación de un equipo de cómputo. Este análisis utiliza como parámetros un tiempo de vida de 5 años tomando como precio de compra el valor máximo del rango mostrado en el análisis comparativo de la tabla 2.

Según el análisis de la depreciación, tomando un tiempo de vida de 3 años para el Cisco 3550, el precio actual del equipo es de $ 1,928.00; acorde a esto, si el equipo se vendiese, el monto obtenido sería suficiente para comprar el 3Com 5500- EI cuyo valor varía entre $ 1,895.00 y $ 2,430.00.

El 3Com 5500 posee características técnicas similares al Cisco 3750 a un menor valor por lo que económicamente es recomendable.

4.4.2. Propuesta para el Router de Núcleo

Como alternativas al Router de núcleo Cisco 2811 se propone el siguiente equipo:

- Router Cisco 2821
- Router 3Com 6080

4.4.2.1. Router Cisco 2821

Figura 14: Router Cisco 2821

Posee la capacidad de entregar múltiples servicios de alta calidad simultáneamente a altas velocidades hacia conexiones T1/E1/xDSL. El router Cisco 2821 ofrece encriptación embebida y en la tarjeta madre ranuras para procesador de señal digital de voz (DSP); sistema de prevención de intrusos (IPS) y funciones de firewall; interfases de alta densidad

para un amplio rango de requerimientos de conectividad por cable e inalámbrico; capacidad para futuras expansiones en la red y aplicaciones avanzadas.

Características del equipo:

- Memoria RAM de 256 Mb hasta 1 Gb.
- Memoria Compact Flash de 64 Mb hasta 256 Mb.
- 2 puertos USB.
- 2 puertos 10/100/1000.
- 2 ranuras internas AIM.
- 4 ranuras para tarjetas de interfase HWIC, WIC, VIC, VWIC.
- 1 ranura para modulo de red NM, NME o NME-X.
- 1 ranura para modulo de voz.
- 3 ranuras PVDM (DSP).
- 1 puerto para administración
- 1 puerto auxiliar
- 1 puerto para RPS

Características especiales:

- Alto rendimiento para servicios concurrentes como seguridad y voz y para servicios avanzados a múltiples rangos.
- Incremento de la densidad a través de las ranuras para tarjetas de interfase de alta velocidad.
- Soporta sobre 90 módulos existentes o nuevos.
- Soporta Power over Ethernet (PoE) en Layer2 (opcional).
- Seguridad:
    - Encriptado por hardware.
    - Soporta hasta 1500 túneles VPN con el módulo AIM – EPII – PLUS.
    - Soporte de antivirus a través del Network Admission Control (NAC).

- Voz:
    - Soporte de llamadas de voz análoga y digital.
    - Soporte correo de voz opcional.

4.4.2.2. Router 3Com 6080

Figura 15: Router 3Com 6080

El 3Com 6080 es un router de 8 ranuras flexible que presenta conectividad WAN. Con fuente de poder y ventilador integrados tiene la capacidad de instalación para una segunda fuente de poder. Se integra con la Unidad de Procesamiento 3Com que tiene dos puertos LAN 10/100 y provee función habilidad de ruteo con soporte para IP/IPX, MPLS, OSPF, RIP V1/V2, IS-IS, ruteo BGP-4, QoS, Multicast, VPN y Firewall.

Características de equipo:

- Procesador a 733 Mhz.
- 512 Mb de RAM.
- 32 Mb Memoria Flash.
- 2 puertos 10/100 Base – TX.
- 1 puerto serial.
- 1 puerto de administración.
- 9 ranuras de expansión.
- Rango de transferencia de datos de 100 Mbps.
- Protocolo de vinculo de datos Ethernet/Fast Ethernet.
- Fuente de poder interna redundante.

Características especiales:

- Interfaces WAN: Frame relay, ISDN PRI, X.25, E1/E3, T1/T3, V.24, V.35, X.21, HDLC/SDLC, síncrono, asíncrono, ATM, ADSL.
- Ruteo IP, IPX, RIP V1/V2, OSPF, BGP-4, MPLS, IS-IS integrado (IP), Multicast.
- Seguridad: VPN (L2TP, GRE, IPSec), MPLS VPN, firewall, ACLs, NAT, RADIUS, PAP/CHAP, encriptación (DES, 3DES, AES).
- Convergencia de datos: Calidad de servicio (QoS), Multicast (IGMP, PIM-SM, PIM-DM), IEEE 802.1q VLAN, ruteo Inter-VLAN, multilinks.
- Confiabilidad: Módulos hot-swap, fuente de poder redundante, imagines de software duales; VRRP (Virtual Router Redundancy Protocol), Backup (Configuration / Port), multilink.
- Administración vía CLI, Telnet, SSH, reverse Telnet, Puerto de consola, Rlogin, y SNMP.

4.4.2.3. Análisis comparativo

A continuación se muestra un cuadro comparativo de las características[4] del equipo que actualmente se esta utilizando con las del equipo propuesto.

Tabla 4: Análisis técnico comparativo de routers propuestos

	Cisco 2811	Cisco 2821	3Com 6080
Procesador	n/a	n/a	1 x 733 Mhz
Memoria RAM	256 – 760 MB	256 MB – 1GB	512 MB
Memoria Flash	64 – 256 MB	64 - 256 MB	32 MB
Rango de Transferencia de Datos	100 Mbps	100 Mbps	100 Mbps
Protocolo Data Link	Ethernet, Fast Ethernet	Ethernet, Fast Ethernet, Gigabit Ethernet	Ethernet, Fast Ethernet
Protocolo de red/transporte	IPSec	IPSec	n/a
Protocolo de Administración Remota	SNMP3	SNMP3	SSH, CLI, Telnet, SNMP, RLOGIN.
Tecnología de Conectividad	Cableado	Cableado	Cableado

[4] Características basadas en configuración de fábrica.

Características	Protección Firewall, encriptado por hardware, VPN, soporte MPLS, filtrado URL	Protección Firewall, encriptado por hardware, VPN, soporte MPLS, filtrado URL	Administrable
Estándares compatibles	IEEE 802.3af	IEEE 802.3af	IEEE 802.1Q
Ranuras de expansión libres	1 x NME 4 x HWIC 2 x AIM 2 x PVDM 1 memoria 1 tarjeta CompactFlash	4 x HWIC 2 x AIM 1 x NME-X 1 x EVM 3 x PVDM 2 memoria 1 tarjeta CompactFlash	9 x FIC
Interfase	2 x red - Ethernet 10Base-T/100Base-TX 2 x USB 1 x administración - consola 1 x serial - auxiliar 1 x modem - SHDSL	2 x red - Ethernet 10Base-T/100Base-TX/1000Base-T 2 x USB 1 x administración - consola 1 x red - auxiliar	2 x red - Ethernet 10Base-T/100Base-TX 1 x serial 1 x administración
Algoritmo de encriptación	DES, Triple DES, AES	DES, Triple DES, AES	DES, Triple DES, AES
Dispositivo de poder	Fuente interna	Fuente interna	Fuente interna
Voltaje requerido	n/a	DC -24/-60 V	AC 120/230 V (50/60 Hz)
Garantía	De por vida	De por vida	1 año
Temperatura de operación mínima	32 F	32 F	32 F
Temperatura de operación máxima	104 F	104 F	104 F
Rango de humedad operacional	5 - 95%	5 - 95%	5 - 90%
Rango de Precio	$ 2,156.41 – 2,467.86	$ 3,039.15 – 3,619.42	$ 5,383.94 – 6,580.00

Como se observa en la tabla 4, los equipos propuestos mantienen similares características o mejoran levemente al equipo que actualmente se esta utilizando.

Ventajas que proporciona el Cisco 2821:

- Mayor capacidad de memoria.
- Capacidad para soportar redes Gigabit Ethernet.
- Más capacidad para tarjetas de expansión.

Las desventajas que se encuentran en este equipo son las siguientes:

- Carece de interfase para modem.
- Mayor costo del equipo.

Entre las ventajas que proporciona el 3Com 6080 se tienen:

- Alta velocidad de procesamiento.
- Mayor capacidad de memoria.
- Compatibilidad con más protocolos de administración.
- Ranuras para tarjetas de expansión Hot-Swap.

Las desventajas del 3Com 6080 son las siguientes:

- Requiere integrarse a un modulo de procesamiento externo.
- Mayor costo del equipo.

4.4.2.4. Recomendación técnico financiera

En el caso del router, el equipo recomendado no mejora significativamente las características que posee el equipo actual; adicionalmente el equipo actual posee la capacidad de implementación de las tecnologías derivadas de las redes avanzadas, como lo son QoS, Ipv6 y Multicast.

Por lo mencionado anteriormente no se recomienda su reemplazo a menos que sea por algún daño interno o externo.

Tabla 5: Análisis financiero de la depreciación del Cisco 2811

Años de uso	Valor a depreciar (precio original)	Depreciación	Saldo a depreciar (precio actual)	Depreciación acumulada
1	$ 2,467.86	$ 493.57	$ 1,974.29	$ 493.57
2	$ 2,467.86	$ 493.57	$ 1,480.72	$ 987.14
3	$ 2,467.86	$ 493.57	$ 987.14	$ 1,480.72
4	$ 2,467.86	$ 493.57	$ 493.57	$ 1,974.29
5	$ 2,467.86	$ 493.57	$ 0.00	$ 2,467.86

La tabla 5 muestra el análisis financiero de la depreciación de un equipo de cómputo. Este análisis utiliza como parámetros un tiempo de vida de 5 años tomando como precio de compra el valor máximo del rango mostrado en el análisis comparativo de la tabla 4.

Según el análisis de la depreciación, tomando un tiempo de vida de 3 años para el Cisco 2811, el precio actual del equipo es de $ 987.14; acorde a esto, si el equipo se vendiese, el monto obtenido sería insuficiente para comprar cualquiera de los equipos recomendados.

Ninguno de los equipos recomendados supera significativamente las características del Cisco 2811 y adicionalmente, ambos equipos cuestan mucho más que el equipo actual. Por esto, económicamente, no es recomendable sustituir el equipo actual.

4.1. RECOMENDACIÓN PARA LA IMPLEMENTACIÓN DE LA RED AVANZADA

En base a los análisis técnico–financieros anteriormente explicados, la recomendación para la implementación de la red avanzada en la Universidad Don Bosco es la siguiente:

Para el switch de núcleo se recomienda cambiar el actual equipo Cisco 3550 Catalyst por el 3Com 5500-EI. Esto debido a que mejora de forma notable las características del equipo actualmente en uso y tiene la capacidad de implementar Multicast, Calidad de Servicio e Ipv6. También es el que tiene el menor costo.

Respecto a los adaptadores necesarios para convertirlo al estándar de fibra óptica 100 Base-Fx, estos se encuentran en el mercado con valor entre $102.99 a $199.98 cada uno, representando aproximadamente $2884.00 por los

28 adaptadores, que sumándolo al valor[5] del equipo aún representa un menor costo comparado con el Cisco 3750 Catalyst.

Para el caso del router de núcleo, el Cisco 2811 no se recomienda que se sustituya en este momento ya que actualmente cumple con los requisitos necesarios para el tamaño de la red además de soportar Multicast, Calidad de Servicio e Ipv6. La sustitución de este equipo esta sujeta a la oferta en el mercado de un equipo que mejore sus características técnicas por medio del soporte de nuevas tecnologías derivadas de las redes avanzadas a un bajo costo para la Universidad Don Bosco.

Esta recomendación preparará la infraestructura de la red avanzada de la Universidad Don Bosco para soportar la implementación de Ipv6, Multicast y Calidad de Servicio cuando sea requerido.

4.2. REQUERIMIENTOS PARA IMPLEMENTAR UNA RED AVANZADA

Para hacer una implementación de Red Avanzada primero hay que definir la infraestructura, en este caso se tomará como modelo la Universidad Don Bosco donde ya se está utilizando una red avanzada funcional (ver capítulo 4.3). También se utilizará la configuración de hardware recomendada por CLARA para sus nodos principales (ver capítulo 3.1.3).

El equipo mínimo requerido para una implementación es como el que muestra la tabla 6.

Tabla 6: Equipo básico para implementar una red avanzada

NOMBRE DEL EQUIPO	EQUIPO MÍNIMO RECOMENDADO	CANTIDAD	PRECIO UNITARIO
Router de núcleo	Cisco 2610	1	$ 725.00 - 1,500.00/unidad
Switch de núcleo	Cisco 3550 Catalyst	1	$ 3,735.99 - 4,819.99/unidad
Convertidor de medios	Allied Telesyn MC101XL	2	$ 149.99 – 187.96/unidad
Cable UTP	Categoría 5e	n/a	$ 0.17 - 2.99/pie
Cable Fibra Óptica	Fibra Multimodo	n/a	$ 3.03 - 32.99/metro

[5] Menor precio mostrado en el análisis comparativo de la Tabla 2.

Además de este equipo es necesario contar con el servicio de Internet Dedicado, proporcionado por la empresa que posea el acceso al nodo de RedClara, en este caso la empresa de telecomunicaciones Telecom. El precio de este servicio depende de la velocidad solicitada según la tabla 7.

Tabla 7: Precio mensual de Internet dedicado según velocidad

VELOCIDAD EN Kbps	CONTRATO DE 1 AÑO	CONTRATO DE 2 AÑOS	CONTRATO DE 3 AÑOS
128	$ 199.00	$ 189.00	$ 179.00
256	$ 250.00	$ 237.00	$ 225.00
384	$ 350.00	$ 332.00	$ 315.00
512	$ 400.00	$ 380.00	$ 360.00
768	$ 700.00	$ 665.00	$ 625.00
1024	$ 810.00	$ 769.00	$ 729.00
2048	$ 1,000.00	$ 950.00	$ 900.00

Debido a que el acceso a las Redes Avanzadas es restringido a instituciones educativas y ciertas organizaciones sin fines de lucro, para funciones de investigación de tecnología y educación, su instalación y configuración no es una oferta comercial.

Lo anterior obliga a que la institución que desee integrarse a RedClara debe proporcionar el personal técnico que será encargado de instalar y dar el mantenimiento respectivo a la Red Avanzada. Este personal es capacitado por medio del grupo RAICESTEC que es conformado por el NOC y el NEG de RAICES y que actualmente esta a cargo de la Universidad Don Bosco.

La estructura básica de una implementación de Red Avanzada debe ser similar a la mostrada en la figura 16.

Como se observa en la figura 16, la señal de la Red Avanzada, luego de llegar al Switch Cisco 3550, es distribuida a la red o redes locales de la institución. Esto permite que estas LAN puedan acceder a la RedClara por medio del nodo principal de México, que es al que esta conectada la red de El Salvador.

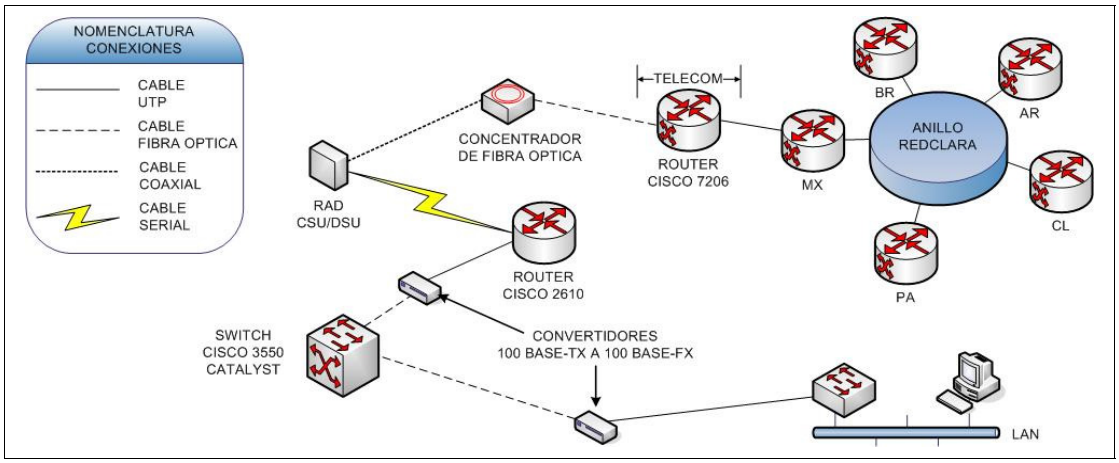


Figura 16: Esquema básico de conectividad a la Red Avanzada

Si una institución desea implementar el esquema antes descrito para poder acceder a las Redes Avanzadas, el gasto de instalación promedio será como el que se muestra a continuación:

Tabla 8: Gasto promedio de instalación de una Red Avanzada

EQUIPO	PRECIO[6]	CANTIDAD	TOTAL
Router	$ 1,112.50	1	$ 1,112.50
Switch	$ 4,277.99	1	$ 4,277.99
Convertidor de medios	$ 168.98	2	$ 337.96
Cable UTP	$ 1.58	328 pies[7].	$ 518.24
Cable Fibra Óptica	$ 18.01	10 mts.	$ 180.10
		TOTAL INSTALACION	$ 6,426.79

El gasto mensual en el que incurrirá la institución luego de realizar la instalación de la red, es el pago del servicio de conexión dedicada y el sueldo del personal encargado de configurar y dar mantenimiento a la red.

Este gasto depende del ancho de banda (cantidad de Kbps) que la institución desee utilizar según sus necesidades y el pago del personal dependerá de las negociaciones respectivas.

[6] Valores promedio basados en información de equipo y precios de Tabla 6.
[7] Valor estimado equivalente a 100 metros.

Capítulo 5

Integración de la red avanzada en la Universidad Don Bosco

La Internet de hoy en día ya no es una red académica, como en sus comienzos, sino que se ha convertido en una red que involucra, en gran parte, intereses comerciales y particulares. Esto la hace inapropiada para la experimentación y el estudio de nuevas herramientas en gran escala.

Adicionalmente, los proveedores de servicios sobre Internet "sobre venden" el ancho de banda que disponen, haciendo imposible garantizar un servicio mínimo en horas pico de uso de la red. Esto es crítico cuando se piensa en aplicaciones propias de redes avanzadas, que requieren calidad de servicio garantizada.

Por otro lado, los enlaces de alta velocidad son aún demasiado costosos para poder realizar su comercialización masiva.

Todo esto, nos lleva a la conclusión que Internet no es un medio apto para dar el salto tecnológico que se necesita para compartir grandes volúmenes de información, videos, transmisión de conferencias en tiempo real o garantizar comunicación sincrónica permanente.

5.1. LA RED INTERNET Y LA RED AVANZADA

El funcionamiento de la Red Avanzada en comparación con Internet es muy similar, inclusive, pueden compartir los mismos medios de comunicación (fibras, routers, y otros). La diferencia primordial entre la red Internet y la Red Avanzada es el uso que se les da; mientras la primera tiene, fundamentalmente, un uso comercial, informativo y de entretenimiento; la segunda es una red de usos educativos, de colaboración científica y de investigación, por este motivo, la divulgación del conocimiento y el aprendizaje constituyen sus principales objetivos.

Otra diferencia importante es que las redes avanzadas, muchas de ellas son administradas por universidades, lo que permite que sea la misma comunidad la que defina la forma de operación y los protocolos que deberán ser soportados en ellas, sin tener que esperar a que éstos sean soportados y requeridos por un gran número de usuarios; ejemplo de estos protocolos son Multicast e IPv6, donde el primero ha servido para la creación de access-grid (transmisión de hasta 100 sitios de videoconferencia, transmisión de video de alta calidad, grids de súper cómputo).

Debido al gran éxito que la Red Avanzada ha tenido en algunos países, las comunidades han ido más lejos y han decidido adquirir sus propias fibras ópticas (dark fibers), lo cual les permite que sean ellos quienes definan los anchos de banda de sus redes, pudiendo crear redes con grandes anchos de banda de 1 a 10 gigabits o, incluso, superiores usando técnicas como DWDM

(*Dense Wavelength Division Multiplexing*, *Multiplexación por división en longitudes de onda densas*), en la cual, se hace uso de varios láser de diferentes longitudes de onda; con esta última tecnología, no sólo se está limitando a la creación de redes IP. DWDM permite crear redes con cualquier tecnología óptica, como ejemplo fiber-channel, con la cual, se pueden crear redes de almacenamiento masivo (SAN, Store Area Network), que al tener sus propias fibras, puede crear una red de almacenamiento masivo distribuida geográficamente, uniendo varias SAN y con ello sumando las capacidades existente de todas. En Estados Unidos de Norteamérica existe el proyecto llamado HOPI[8] (Hybrid Optical and Packet Infrastructure Project, Proyecto de infraestructura híbrida de óptica y paquetes).

En cuanto a la infraestructura física de las redes, la Red Avanzada fue creada para ser una red de alto desempeño con la finalidad de satisfacer las demandantes aplicaciones que serán transportadas por ella. Está sustentada en tecnologías de vanguardia que permiten una alta velocidad en la transmisión de contenidos y que funcionan independientes de la Internet comercial actual.

Uno de sus principales objetivos es desarrollar la próxima generación de aplicaciones telemáticas; estas son aplicaciones que utilizan las facilidades de telecomunicación e informática.

Las redes avanzadas no son solamente sinónimo de grandes anchos de banda o de altos rendimientos, sino que además de la posibilidad de manejar mayores velocidades de transmisión cuentan con otros atributos, como lo son:

- Multicast.
- Calidad de Servicio (QoS).
- Protocolos especializados (Vgr. H.323).
- Ipv6

[8] http://networks.internet2.edu/hopi/

5.2. PROTOCOLO DE INTERNET MULTICAST

Internet Protocol (IP, Protocolo de Internet) Multicast es una tecnología de conservación de ancho de banda que reduce el tráfico entregando simultáneamente una sola cadena de información a miles de destinatarios corporativos y usuarios finales. Aplicaciones que toman ventaja de multicast incluyen videoconferencia, comunicaciones corporativas, aprendizaje a distancia, distribución a distancia, bolsa de valores, noticias.

IP Multicast entrega el tráfico desde el origen a múltiples receptores sin agregar alguna carga adicional al origen o a los receptores mientras se utiliza el menor ancho de banda. Los paquetes multicast son replicados en la red por routers habilitados con protocolos que soporten multicast resultando en la más eficiente entrega de datos a la mayor cantidad de receptores posible.

Todas las actuales alternativas requieren del origen enviar más de una copia de los datos. Algunas hasta requieren del origen enviar una copia individual de los datos a cada destinatario. Aplicaciones que utilizan grandes anchos de banda, como video MPEG, pueden requerir una larga porción del ancho de banda disponible en la red para una sola cadena de datos. En estas aplicaciones, la única manera de enviar a más de un destinatario simultáneamente es por medio de IP Multicast. La figura 17 muestra como la información de un origen es entregada a varios destinatarios utilizando IP Multicast.

Multicast esta basado en el concepto de un grupo. Un grupo arbitrario de receptores expresa un interés en recibir una cadena de datos en particular. Este grupo no tiene ninguna relación física o geográfica, estos “huéspedes” pueden estar localizados en cualquier parte en Internet. Cualquier huésped que este interesado en recibir el flujo de datos desde un grupo en particular debe unirse al grupo por medio de IGMP (Internet Group Management Protocol,

Protocolo de administración de grupo en Internet), en pocas palabras, el huésped debe ser miembro del grupo para recibir la cadena de datos.

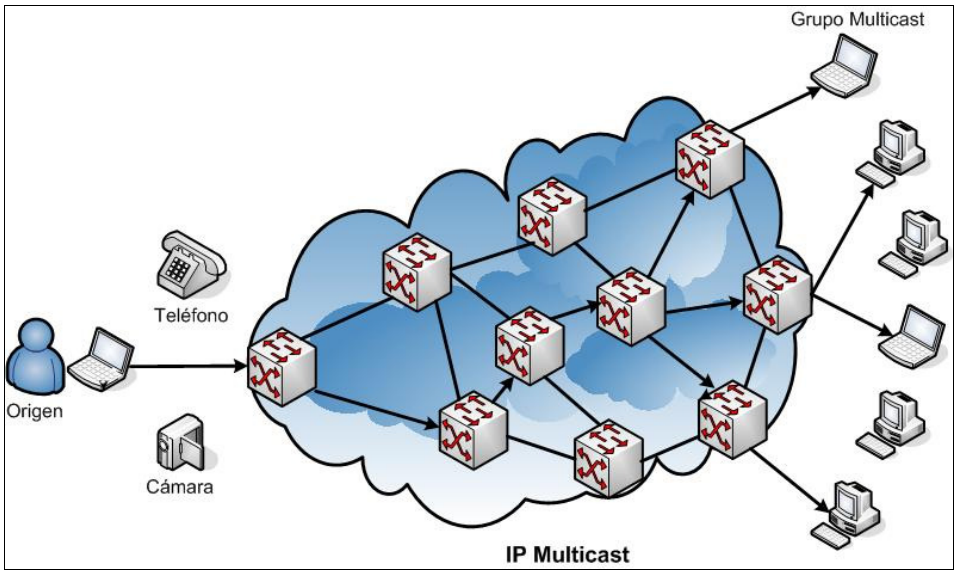


Figura 17: Envío de paquetes a varios destinatarios usando multicast.

Internet Group Management Protocol

IGMP es usado para registrar dinámicamente huéspedes individuales en un grupo multicast en una LAN en particular. Los huéspedes identifican la membresía grupal enviando mensajes IGMP a su router multicast local. Bajo IGMP, los routers escuchan estos mensajes y periódicamente envían consultas para descubrir cuales grupos están activos o inactivos en una subred en particular.

Existen dos versiones de IGMP, IGMPv1 e IGMPv2. Ambas versiones funcionan básicamente igual. La diferencia principal es que en IGMPv2 existe un mensaje de despedida que el huésped comunica cuando deja el grupo multicast. El router luego envía una consulta al grupo y determina si hay huéspedes restantes interesados en recibir las cadenas de datos. Si no hay

respuesta, el router desconecta al grupo y detiene el tráfico. Esto reduce grandemente el tráfico innecesario en la red.

Las características propias de ambos protocolos se definen en el RFC1112 para IGMPv1 y el RFC2236 para IGMPv2.

5.2.1. Diferencias entre Unicast y Multicast

Multicast es la tecnología para enviar paquetes con una dirección especial de destino llamada "dirección grupal" hacia múltiples nodos participando en este grupo. Al contrario de la transmisión de paquetes repetitiva de unicast hacia múltiples nodos, el nodo transmisor necesita enviar el paquete multicast solamente una vez para alcanzar múltiples destinatarios.

Comparado con la transmisión repetitiva unicast, la transmisión multicast tiene las siguientes ventajas:

- La transmisión de paquetes necesita ser hecha solamente una vez.- El nodo transmisor necesita enviar paquetes solamente una vez. Esto conduce a reducir la carga para el transmisor y la red. También contribuye a mantener el tiempo real en la transmisión de datos.
- Fácil administración de direcciones.- El nodo transmisor solamente necesita conocer la dirección grupal. Puede conducir la comunicación sin saber la dirección de los nodos receptores.

Las desventajas de multicast son:

- No puede ser aplicado para comunicaciones TCP.- Pero se puede acercar al concepto de comunicación TCP por medio de tecnología para prevención de perdida de paquetes como Forward Error Correction (FEC) o tecnología de administración de ancho de banda como Datagram Congestion Control Protocol (DCCP).

- Todos los routers necesitan soportar multicast.- Todos los routers en la red multicast necesitan ser capaces de difundir paquetes multicast.

Con estas características, las comunicaciones multicast son usadas a menudo para aplicaciones broadcast como streaming, y protocolos de detección de servicios como el Neighbor Discovery Protocol (NDP) o protocolos de control de rutas.

5.2.2. Componentes Multicast

La comunicación multicast esta compuesta por el nodo transmisor, los nodos receptores y los routers intermedios. Aunque no necesariamente, la Ethernet juega un papel importante en el multicast.

Nodo transmisor

El nodo transmisor envía los paquetes IP a las redes como una transmisión unicast normal. La única diferencia es que la dirección grupal, una dirección especial para multicast, como la dirección destino.

Router

Luego de recibir los paquetes multicast desde el nodo transmisor, el router los envía a todas las interfases para que alcancen los nodos receptores. Múltiples copias son hechas de un paquete, para enviar a más de una interfase. Cuando el router difunde los paquetes multicast, se refiere a la tabla de ruteo multicast para determinar las interfases de salida.

La tabla de ruteo multicast es diferente de la tabla de ruteo unicast, en que contiene información del nodo transmisor así como de la dirección grupal. Esto es porque los paquetes de la misma dirección multicast pueden ser enviados a diferentes routers, dependiendo del nodo transmisor.

Los routers utilizan dos protocolos para construir las tablas de ruteo multicast. Uno es el router-host protocol, es cual es utilizado por el router para aprender sobre las solicitudes de los nodos receptores. El otro es el router-router protocol, con el cual los routers intercambian las solicitudes multicast obtenidas por medio del router-host protocol, para determinar como difundir los paquetes multicast.

Ethernet

Cuando los routers envían los paquetes a las interfases Ethernet, las características del medio Ethernet ofrecen ventajas significativas a las comunicaciones multicast. Si el destino de una trama Ethernet tiene una dirección física en la cual el sexto bit del primer octeto es "ON", entonces la trama es difundida a todos los nodos en la misma red Ethernet, sin importar los protocolos de los layer más altos.

Nodo Receptor

El nodo receptor considera todos los paquetes enviados a la dirección grupal multicast como destinados a él mismo y los recibe.

El nodo receptor utiliza el host-router protocol para enviar la solicitud de ingreso multicast para su propia dirección de red, cuando desea comenzar a recibir paquetes de un grupo multicast específico. Con multicast, a diferencia de unicast, el nodo receptor necesita recibir paquetes con la dirección destino que es diferente a su propia dirección. Por lo tanto, las terminales receptoras necesitan enviar la solicitud de ingreso a la red antes de comenzar a recibir los paquetes multicast.

5.2.3. Protocolos de enrutamiento multicast

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

- Protocolos de Modo Denso: entre estos protocolos se encuentran el DVMRP y PIM-DM.
- Protocolos de Modo Disperso: como el PIM-SM.
- Protocolos de Estado de Enlace: entre los que se encuentra el MOSPF.

Protocolos como el PIM-SM construyen diferentes tablas de enrutamiento multicast para diferentes volúmenes de paquetes: RP Tree (RP), Register-Stop (RS) y Shortest-Path Tree (SPT).

RP Tree (Rendezvous Point Tree, Árbol de punto de reunión)

Este es un patrón donde los paquetes multicast son enviados a un router PIM-SM (RP, Punto de reunión) por unicast y luego reenviado a los destinos actuales desde el router RP. Los paquetes son encapsulados por unicast en paquetes PIM Register. Luego el router en el destino desencapsula los paquetes que recibe.

Register-Stop (RS, Registro de parada)

Este es similar al RP Tree, pero en este caso, la transmisión de datos para el router RP es enviado sobre multicast, sin encapsular. Los paquetes enviados desde el router de origen forman una ruta multicast hasta el router destino. Cuando los paquetes llegan al router RP, este envía un mensaje PIM Register-Stop para solicitar el fin del túnel para los paquetes PIM-Register. Esto permite que los paquetes enviados a través del router RP viajen sin ser encapsulados.

Shortest-Path Tree (SPT, Árbol más corto)

Este es para transmisión de paquetes multicast con el camino más corto (Shortest-Path) desde el transmisor hasta los receptores. Por medio de

mensajes de “unión” y “supresión” entre la dirección de origen a través del router RP hasta el router destino se crea la tabla de ruteo multicast que habilita el envío multicast por medio del shortest-path.

5.2.3.1. Protocolos de modo denso

Los protocolos del tipo “Dense Mode” (DM) utilizan el árbol más corto junto con un mecanismo de empuje (push). Este mecanismo de empuje asume que en cada interfaz del router existe al menos un receptor del grupo. El tráfico es enviado o “flooded” a través de todas las interfaces. Para evitar el desperdicio de recursos, si un router no desea recibir tráfico envía un mensaje de supresión (prune). Como resultado se tiene que el tráfico de multicast sólo es enviado a los router 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. Protocolos basados en modo denso son el Distance Vector Routing Protocol (DVMRP) y el Protocol Independent Multicast Dense Mode (PIM-DM).

Distance Vector Multicast Routing Protocol (DVMRP):

- Primer protocolo de enrutamiento desarrollado para multicast y que tuvo un uso masivo.
- DVMRP - Distance Vector basado en RIP, tiene todas las desventajas de los Distance Vector.
- Updates Periódicos (cada 60 segundos).
- 32 brincos máximo.
- “Classless”.
- Dense Mode.
- No es escalable.

- No se recomienda su uso en las redes multicast actuales.

Protocol Independent Multicast Dense Mode (PIM-DM):

- Tipo Dense Mode, "flood" cada 3 minutos.
- No se recomienda para ambientes WAN.
- Independiente de protocolo de enrutamiento de unicast.
- Sencillo de configurar.
- No se recomienda por su comportamiento de "flood" saturando la red de forma innecesaria.

5.2.3.2. Protocolos de modo disperso

Los protocolos del tipo "Sparse Mode" (SM) hacen uso del modelo de árboles compartidos y ocasionalmente como el PIM Sparse Mode (PIM-SM) del "Short Path Tree" (SPT) para la distribución de tráfico multicast. Al contrario de los DM, los SM hacen uso de un mecanismo de jale (pull). 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 router receptor debe enviar a la raíz u origen una solicitud de unión al árbol (Join message). Este mensaje viaja de router a router 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 jale, 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 "Rendezvous Point" (RP) ya que si este 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 Tree) para una fuente en particular.

Protocol Independent Multicast Sparse Mode (PIM-SM):

- Tipo Sparse, no genera tráfico a menos que se solicite.
- Se recomienda para ambientes WAN y LAN.
- Independiente de protocolo de enrutamiento de unicast.
- Sencillo de configurar pero requiere de un Redenvouz Point (RP), este puede ser aprendido de modo automático mediante Auto-RP o Bootstrap Router (BSR).
- Se recomienda para la arquitectura de las redes avanzadas.

5.2.3.3. Protocolos de estado de enlace

Los protocolos de estado de enlace como Multicast Open Short Path First (MOSPF) hacen uso del "Short Path First" (SPF). Para construir estos árboles, los router envían información de estados de enlace que identifica la ubicación en la red de los grupos de miembros de multicast. Con esta información los router forman un SPT de cada fuente hacia todos los receptores en el grupo.

Multicast Open Short Path First (MOSPF):

- Basado en OSPF.
- Debe construir árboles de expansión para construir árboles más cortos.
- OSPF debe estar configurado.
- Utiliza mucho CPU de router si la topología cambia constantemente.
- Su escalabilidad es cuestionable.
- No ha sido ampliamente usado.
- Complejo.

- No se propone para la red avanzada pero se puede considerar como alternativa.

5.2.3.4. Otros protocolos multicast

Multicast Border Gateway Protocol (MBGP):

- Permite usar los mismos comandos de "peering" de BGP, lo cual reduce la curva de aprendizaje.
- Permite que el tráfico de multicast y unicast puedan usar caminos (paths) diferentes. Topologías no congruentes.
- Si las topologías son congruentes los caminos de multicast y unicast pueden tener políticas diferentes.
- Permite anunciar alcanzabilidad de fuentes de multicast para el Reverse Path Forwarding (RPF).

Multicast Source Discovery Protocol (MSDP):

- Permite que los RPs en diferentes dominios de Multicast (AS) sean independientes unos de otros.
- Muy útil en Multicast Inter-domain.
- Permite descubrir las fuentes de Multicast de otros dominios.

5.2.4. Recomendación para el uso de protocolos de enrutamiento en la red avanzada

Para la arquitectura de IP multicast, se sugiere el uso de PIM Sparse Mode. Con PIM-SM se eliminará el innecesario tráfico de multicast por los enlaces WAN. Se recomienda además que los RP sean descubiertos de forma automática por los router de tal forma que el proceso sea más eficiente y a prueba de fallas. El protocolo que se recomienda para esta actividad es el

Bootstrap Router (RFC2362, PIMv2). Aunque este protocolo es un poco más complejo que el Auto-RP (propietario de Cisco) asegura la interoperabilidad con routers de otras marcas. Esto además de evitar la configuración estática de los RPs, asegura una redundancia en caso de falla de los RPs.

Finalmente se recomienda que las interfaces se configuren como de tipo Sparse-Dense, de tal forma que si todos los RP fallan, la red tenga oportunidad de conmutar a modo denso evitando que se pierda tráfico.

5.2.5. Recomendación para la implementación de multicast en la red avanzada

A continuación se describen ciertos lineamientos básicos para la implementación de IP-Multicast en una red local y su conexión a un backbone de alta velocidad como lo es el de una red avanzada.

Requerimientos básicos

Antes de realizar la implementación se deben tomar en cuenta ciertos requerimientos básicos:

1. Tener un conocimiento al menos básico de IP-Multicast. El grado de dominio de la tecnología está directamente relacionado con el grado de complejidad del ambiente de red en el que se vaya a implementar. Mientras que para una red de un par de routers y switches el grado puede ser básico, para una red de un número grande de routers y switches y/o multiredes el grado de conocimiento deberá ser avanzado.
2. Asegurarse que tanto los routers como los switches de capa 2 soportan IP-Multicast. Para los switches de capa 2 esto es opcional, pero el no soportarlo puede significar un decremento en el desempeño de la red en situaciones de alto tráfico. Es necesario también verificar los “bugs” que

existan en las versiones de sistema operativo de switches y routers para disminuir la posibilidad de falla. Es recomendable actualizar dichos sistemas operativos para corregir estos "bugs".

3. Verificar que los routers además de soportar IP-Multicast soporten PIM Sparse Mode. Aunque esto es opcional se recomienda este protocolo en lugar de DVMRP, MOSPF y PIM Dense Mode.
4. Verificar que los equipos de redes pueden soportar IP-Multicast sin degradar su desempeño. Esto varia dependiendo del tamaño de la red y el número de fuentes de multicast. En general se recomienda una red de multinivel (Capa 3 en core/distribución, Capa 2 en acceso) y sin concentradores de ethernet (hubs), además se recomienda que la capa 2 este basada en la familia Ethernet (Ethernet, Fast Ethernet, Gigabit Ethernet, 10G), esto es porque el IP-Multicast se adapta muy bien a ambientes de red de acceso múltiple al medio con broadcast; mientras que para redes punto a punto, multipunto, o acceso múltiple al medio sin broadcast como ATM y FR es necesario replicar el tráfico a un punto central, el cual puede convertirse en un cuello de botella. Esto puede resolverse si la red esta basada en routers con ATM/FR y no en switches de capa 2, esto, sin embargo no es común en redes locales.
5. Si planea conectarse a las redes avanzadas, además es necesario tener un enlace a RedClara, intercambiar tráfico por BGP y que el router con la conexión soporte Multicast Border Gateway Protocol (MBGP) y Multicast Source Discovery Protocol (MSDP).

Diseño

Para que el IP-Multicast funcione correctamente y se aprovechen todas las capacidades de la red es necesario partir de un buen diseño. Para esto es necesario conocer a detalle las capacidades de la red; donde se encuentran los equipos de más alto desempeño, los de más bajo desempeño, los segmentos de

la red con baja capacidad, segmentos con switches sin soporte de multicast y/o concentradores, segmentos con tecnología ATM, etc.

Después de conocer las capacidades de la red, es necesario decidir donde se habilitará IP-Multicast, esto depende de donde estarán los receptores de sesiones y las fuentes de sesiones.

Para el caso de las fuentes de sesiones, se recomienda que estén cerca de los puntos centrales de la red de forma que tengan que atravesar el menor número de brincos para llegar a los receptores en la LAN o en la Red Avanzada.

Un punto crítico en el diseño es decidir el protocolo de enrutamiento de IP-Multicast. El recomendado en este caso es el PIM-Sparse Mode.

Para PIM-Sparse Mode es necesario primero decidir si se usarán Redenvouz Point (RP) estáticos o dinámicos. Para el caso de dinámicos existen dos opciones, Auto RP y Bootstrap RP. Auto RP es una implementación propietaria de Cisco Systems y Bootstrap RP es parte del estándar definido para la versión 2 de PIM-Sparse Mode.

Implementación

A continuación se presenta una guía general de implementación. Se recomienda seguirla en el orden que se indica, sin embargo algunos puntos pueden hacerse antes que otros si se conoce la razón de hacerlo, y si el punto es opcional, se indicará.

1) Habilitar ruteo de multicast en routers.
2) Para RP-estáticos:
    a. Configurar en cada router la IP del RP.

   b. Configurar las interfases de interconexión, usuarios y fuentes con PIM-Sparse Mode.
   c. Pasar al punto 5.

3) Para Auto RP:
   a. Configurar un router como RP.
   b. Configurar las interfases de interconexión, usuarios y fuentes con PIM-Sparse-Dense Mode.
   c. Pasar al punto 5.
4) Para Bootstrap RP:
   a. Configurar un router como RP.
   b. Configurar las interfases de interconexión, usuarios y fuentes con PIM-Sparse Mode.
   c. Pasar al punto 5.
5) Si se tienen routers y switches Cisco habilitar CGMP (Cisco Group Management Protocol), opcional si no se quiere inundar los puertos de los switches de capa 2 con tráfico de multicast como si fuera broadcast.
6) Habilitar IGMP Snooping. Opcional como el punto 5. Si se habilita CGMP no es necesario.
7) Poner una fuente de multicast y receptores del grupo. Este paso es opcional.
8) Poner filtros de multicast en interfaz de Internet/Red Avanzada según sea el caso.
9) Habilitar MBGP (Multicast Border Gateway Protocol) y MSDP (Multicast Source Discovery Protocol).

5.3. CALIDAD DE SERVICIO (QoS)

La QoS (Quality of Service, Calidad de Servicio) garantiza que se transmitirá cierta cantidad de datos en un tiempo dado (Throughput, rendimiento de procesamiento). Últimamente, han surgido varios mecanismos para ofrecer redes de servicio de calidad (QoS). El principal objetivo de estos

mecanismos es proporcionar un "servicio" de redes mejorado a las aplicaciones en los extremos de la red.

5.3.1. Ventajas de QoS

Los últimos años han sido testigos del rápido crecimiento del tráfico de redes informáticas. Los administradores agregan continuamente nuevos recursos para tratar de responder al ritmo de la creciente demanda. Incluso los clientes de redes no están, a menudo, satisfechos con el rendimiento de la red. El uso creciente de un nuevo tipo de aplicaciones multimedia ávidas de recursos va a agudizar esta situación. Los mecanismos de QoS proporcionan un conjunto de herramientas que el administrador de redes puede utilizar para administrar el uso de recursos de red de una forma controlada y eficaz. Como resultado, se obtendrá un servicio mejor a las aplicaciones y a usuarios de misiones críticas, al mismo tiempo que se va frenando el ritmo al que es necesario aumentar la capacidad. En resumen, QoS puede ayudar a mejorar el servicio a los usuarios de la red, al mismo tiempo que reduce los costos de ofrecer dichos servicios.

A continuación se analizan ejemplos específicos de los beneficios que se pueden esperar como resultado de la implantación de QoS:

Mejor rendimiento de aplicaciones de misiones críticas a través de vínculos de WAN

Las aplicaciones como SAP (software empresarial) o PeopleSoft (E.R.P. - Enterprise Resource Planning) se utilizan, a menudo, para proporcionar servicios de misiones críticas a través de las intranets de área extensa. Estos vínculos son propensos a la congestión, lo que provoca respuestas lentas de la aplicación o tiempos de espera de la sesión que pueden resultar caros. QoS permite al administrador de la red favorecer el tráfico de misiones críticas para que sean inmunes a la congestión de los vínculos de WAN. Esto se puede

conseguir con un costo mínimo para las aplicaciones menos significativas y competitivas. La solución QoS es parecida a proporcionar carriles especiales para cubrir ciertas necesidades en autopistas muy transitadas. El tráfico de estas misiones críticas se desvía a estos "carriles".

Controlar las repercusiones del tráfico multimedia en la red

Las aplicaciones de transmisión multimedia, tales como Windows Media™ Technologies, software de conferencias NetMeeting®, RealAudio y aplicaciones basadas en TAPI 3.0 son cada vez más conocidas entre los usuarios de redes. De esta forma, se generan grandes volúmenes de tráfico UDP. Este tráfico no es muy partidario de las redes en el sentido de que no "da marcha atrás" en caso de congestión. A consecuencia de las posibles repercusiones de este tipo de tráfico en recursos de red, los administradores de redes prohíben o limitan la implementación de aplicaciones multimedia en sus redes. Los mecanismos de QoS permiten al administrador de la red controlar las repercusiones de estas aplicaciones en la red.

Compatibilidad multimedia

El ejemplo anterior ha examinado la utilización de QoS para controlar las repercusiones de las aplicaciones de medios de secuencias en recursos de red sin considerar el servicio que realmente se proporciona a la aplicación multimedia. QoS se puede aplicar para garantizar una calidad de servicio específica a determinadas aplicaciones de medios de secuencias. En este caso, QoS permite convergencia real de redes de multimedia y de datos. Entre las ventajas que ofrece esta convergencia se puede destacar la telefonía IP utilizable con el ahorro proporcional de costos.

5.3.2. Cómo funciona QoS

Las aplicaciones generan tráfico a ritmos variables y requieren normalmente que la red pueda transportar tráfico al ritmo que las aplicaciones

lo han generado. Asimismo, las aplicaciones son más o menos tolerantes a retrasos de tráfico en la red y a variaciones de los mismos. Algunas aplicaciones pueden tolerar cierto grado de pérdida de tráfico, mientras que otras no. Si dispusiéramos de recursos de red infinitos, todo el tráfico de las aplicaciones podría transportarse al ritmo requerido, sin latencia y sin pérdida de paquetes. Sin embargo, los recursos de red no son infinitos. Como consecuencia, hay partes de la red en las que los recursos no pueden responder a la demanda.

Las redes están construidas mediante la unión de dispositivos de red, tales como switches y routers. Estos dispositivos se intercambian el tráfico entre ellos mediante interfases. Si la velocidad en la que el tráfico llega a una interfaz es superior a la velocidad en la que la interfaz puede enviar tráfico al siguiente dispositivo, se produce una congestión. De esta forma, la capacidad de una interfaz para enviar tráfico constituye un recurso de red fundamental. Los mecanismos de QoS funcionan al establecer preferencias en la asignación de este recurso en favor de cierto tráfico.

Para poder realizar esta acción, es necesario, en primer lugar, identificar tráficos diferentes. El tráfico que llega a los dispositivos de red se separa en distintos flujos mediante el proceso de clasificación de paquetes. El tráfico de cada flujo se envía a una cola en la interfaz de reenvío. Las colas de cada interfaz se gestionan de acuerdo con algunos algoritmos. El algoritmo de administración de cola determina la velocidad a la que se reenvía el tráfico de cada cola. De este modo, se determinan los recursos que se asignan a cada cola y a los flujos correspondientes.

Para proporcionar QoS en redes, es necesario configurar y proporcionar a los dispositivos de red lo siguiente:

1. Información de clasificación por la que los dispositivos separen el tráfico en flujos.

2. Colas y algoritmos de administración de cola que controlen el tráfico de los diferentes flujos.

Nos referiremos a ambos como mecanismos de control de tráfico. Los mecanismos de control del tráfico por separado no resultan útiles. Deben proporcionarse o configurarse a través de muchos recursos de una forma coordinada que proporcione servicios de un extremo a otro en una red. Para proporcionar servicios útiles, son necesarios tanto los mecanismos de control de tráfico como los mecanismos de provisión y configuración.

5.3.3. Tecnologías de QoS

A continuación se mencionan los principales mecanismos de control del tráfico y de provisión y configuración.

5.3.3.1. Mecanismos de control del tráfico

Existen varios mecanismos de control del tráfico. Entre estos están: servicios diferenciados (diffserv), 802.1p, servicios integrados (intserv), ATM e ISSLOW. Tenga en cuenta que los mecanismos de control del tráfico se pueden clasificar en mecanismos por conversación o mecanismos por acumulación. Los mecanismos por conversación tratan por separado cada flujo de tráfico para cada conversación. Los mecanismos por acumulación agrupan varios flujos de tráfico en una única clase acumulada. La distinción es parecida al tratamiento de los pasajeros de un avión. Los pasajeros se suelen clasifican en primera clase, clase business y clase turista. Todos los pasajeros de la misma clase tienen el mismo tratamiento. Esto es el tratamiento por acumulación. El tratamiento por conversación es parecido a proporcionar un avión especializado para cada pasajero. Resulta eficiente pero caro.

Servicios diferenciados (Diffserv)

Diffserv es un mecanismo de tratamiento del tráfico por acumulación apropiado para grandes redes enrutadas. Estas redes pueden transportar varios miles de conversaciones. Por tanto, no resulta práctico tratar el tráfico por conversación individual. Diffserv define un campo en los encabezados IP de los paquetes, conocido como DiffServ CodePoint (DSCP). Los host o los routers que envían tráfico a una red diffserv marcan cada paquete transmitido con el valor DSCP. Los routers de una red diffserv utilizan DSCP para clasificar paquetes y para aplicar un comportamiento de cola específico basado en los resultados de la clasificación. El tráfico de varios flujos con requisitos de QoS parecidos se marca con el mismo DSCP, al agregar el flujo a una cola común o al programar el comportamiento.

802.1p

802.1p es un mecanismo de control del tráfico de acumulación apropiado para el uso en muchas redes de área local (LAN).

Define un campo en el encabezado de acceso al medio (MAC) de los paquetes Ethernet, que puede transportar uno de los ocho valores preferentes. Los hosts o los routers que envían tráfico a una LAN marcan cada paquete transmitido con el valor de preferencia adecuado. Los dispositivos LAN, tales como modificadores, puentes o concentradores deben tratar los paquetes de forma adecuada. El ámbito de la marca de preferencia 802.1p está limitado a la LAN.

Servicios integrados (Intserv)

Intserv es una estructura para definir servicios. Como tal, incluye un conjunto de mecanismos de control de tráfico subyacentes. Los servicios Intserv se suelen aplicar por conversación individual. Normalmente, aunque no

de forma necesaria, Intserv se asocia con el protocolo de señalización Resource ReSerVation Protocol (RSVP, Protocolo de reservación de recursos).

ATM, ISSLOW y otros

ATM (Asynchronous Transfer Mode, Modo de Transferencia Asíncrona) es una tecnología de capa de vínculo que ofrece un tratamiento del tráfico de alta calidad. ATM divide los paquetes en celdas de capa de vínculo y, a continuación, se envían a la cola y se controlan con los algoritmos de administración de cola adecuados para uno o varios servicios ATM.

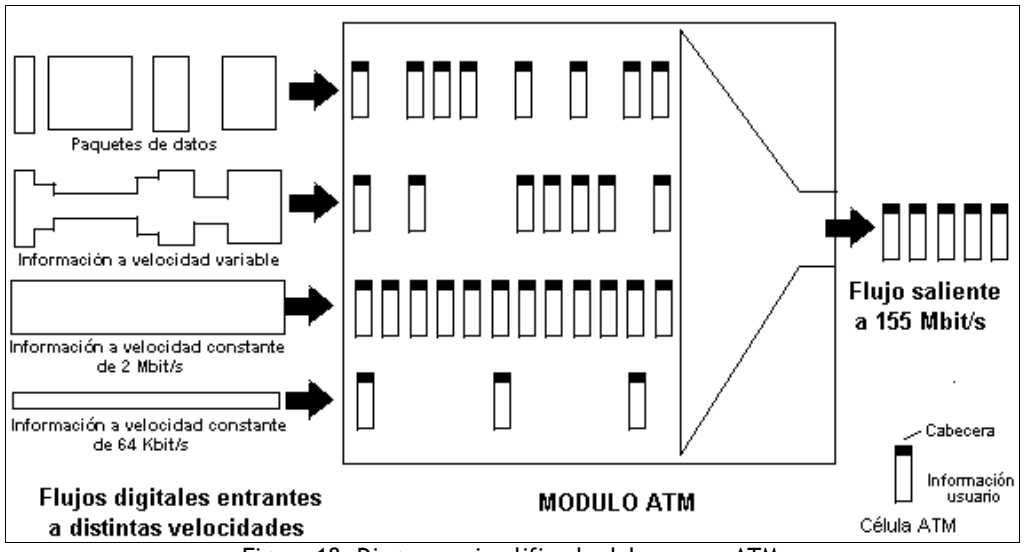


Figura 18: Diagrama simplificado del proceso ATM

ISSLOW (Services Over Slow Link Layers, Servicio sobre capas de vínculo lentas) es una técnica para dividir paquetes IP a medida que se transmiten a través de vínculos de velocidad relativamente lenta, tales como las conexiones telefónicas a módems. Cuando se mezclan datos y sonidos en estos vínculos, las latencias de la señal de audio pueden ser considerables y afectan el uso de la aplicación. Se puede utilizar ISSLOW para reducir las latencias de audio en estas aplicaciones.

Se han definido otros mecanismos de control del tráfico para diversos medios, incluidos módems por cable, plantas coaxiales de fibra híbrida (HFC), P1394, etc. Pueden utilizar mecanismos de señalización de capas de vínculo específicas y de bajo nivel. ATM, por ejemplo, utiliza la señalización User to Network Interface (UNI, Interfaz usuario a red).

5.3.3.2. Mecanismos de provisión y configuración

Para conseguir una provisión efectiva de QoS de red, es necesario desarrollar de forma continua los mecanismos de provisión y configuración del tratamiento del tráfico descrito a través de dispositivos de red múltiples. Se pueden clasificar los mecanismos de provisión y configuración en de arriba a abajo o señalizados.

Provisión de arriba a abajo

En la provisión de arriba a abajo, se utiliza un sistema de administración de red para "insertar" la configuración del tratamiento del tráfico en un conjunto de dispositivos de red. Normalmente, los mecanismos de cola están configurados en interfases de dispositivos. A continuación, se configuran los criterios de clasificación para determinar qué paquetes se envían a cada cola del dispositivo. Los criterios pueden clasificar los paquetes tomando como referencia tupla IP 5 (direcciones y puertos IP de origen y de destino y el protocolo IP) o DSCP y "marcas" de acumulación 802.1p en los encabezados de los paquetes. Se pueden utilizar tuplas 5 con máscara. Los criterios de clasificación pueden especificar sólo un subconjunto de tuplas 5, por ejemplo, "todos los paquetes con una dirección IP de origen de 2.2.2.X", donde "X" puede ser cualquier valor. Si DSCP u 802.1p se especifican como criterios de clasificación, es necesario "señalar" las marcas DSCP u 802.1p en los paquetes en la parte ascendente del dispositivo de clasificación. Los host o los

dispositivos de red que se encuentran cerca del extremo de la red pueden realizar esta acción. En el segundo caso, se configurarían los dispositivos de red de señalización para realizar las marcas tomando como referencia sus propios criterios de clasificación, normalmente, tupla 5 (o algún subconjunto).

Problemas en la provisión de arriba a abajo

Puede resultar complicado determinar los criterios de clasificación adecuados. Los administradores de redes preferirían utilizar QoS para asignar recursos al tráfico de ciertas aplicaciones o usuarios, en lugar de campos en encabezados de paquetes, tales como direcciones o puertos IP. Los sistemas de provisión de arriba a abajo tratan de ayudar al administrador de la red al crear enlaces entre aplicaciones y puertos IP y entre usuarios y direcciones IP. Desafortunadamente, no se puede confiar plenamente en estos sistemas. Las aplicaciones pueden utilizar puertos transitorios o crear un origen común en un puerto para varios flujos de tráfico (que requieren QoS diferentes). Las direcciones IP de los usuarios pueden variar como resultado de DHCP. Los equipos multiusuario pueden utilizar la misma dirección IP para varios usuarios. El cifrado IPSec puede cifrar puertos IP, lo que los convierte en criterios de clasificación que no se pueden utilizar.

Un problema adicional en la provisión de arriba a abajo es la anticipación de los volúmenes de tráfico en varios nodos de la red. Por ejemplo, se puede utilizar un sistema de administración para configurar una cola de baja latencia en cada dispositivo de red, con una capacidad para tratar diez sesiones simultáneas de telefonía IP con ciertos límites de latencia especificados. A continuación, se configuran los criterios de clasificación en cada dispositivo para transmitir el tráfico de telefonía IP a las colas de baja latencia. Este proceso funciona correctamente siempre y cuando el tráfico de telefonía que llega a cada dispositivo esté limitado a diez sesiones. Sin embargo, si se establece una undécima sesión que recorre uno de los

dispositivos configurados, se congestionará la cola de baja latencia y se elevará el nivel de latencia por encima del límite especificado. Como consecuencia, el servicio pondrá en peligro la undécima sesión así como las diez sesiones existentes. Esto se debe a la naturaleza relativamente estática de la provisión de arriba a abajo y al hecho de que el sistema de administración no es directamente compatible con los patrones de tráfico actuales.

Señalización RSVP como mecanismo de configuración

RSVP (Resource ReSerVation Protocol, Protocolo de reservación de recursos) es un mecanismo de configuración señalizado. Es un protocolo por el cual las aplicaciones pueden solicitar a la red QoS fin-a-fin, por conversación, y pueden indicar requerimientos y capacidades QoS para aplicaciones. RSVP es un protocolo de capa 3, adaptado principalmente para usar con trafico IP.

La señalización RSVP se puede utilizar para complementar los mecanismos de provisión de arriba a abajo. En este caso, los hosts generan mensajes de señalización que describen el tráfico de datos relacionado con una conversación en particular. Estos mensajes fluyen por la misma ruta que el tráfico de datos tomaría en la red. Los mensajes RSPV ofrecen la siguiente información a la red:

- Qué soy (origina la aplicación y el subflujo. Por ejemplo, flujo de impresión frente a transacción crítica en el tiempo).
- Quién soy (Id. de usuario autorizado).
- Qué deseo (tipo de servicio QoS necesario).
- Cuánto deseo (ciertas aplicaciones cuantifican los requisitos de recursos de forma precisa).
- Cómo se me puede reconocer (criterio de clasificación de tupla 5 por el que se reconoce el tráfico de datos).

- Qué recursos de dispositivos de red se verán afectados por el tráfico de datos asociado.

La señalización basada en host ofrece ventajas importantes a los sistemas de administración de QoS. Como ventaja evidente se puede destacar que la señalización basada en host proporciona enlaces fuertes entre la información de clasificación y los usuarios y las aplicaciones. Además, este tipo de señalización ofrece control de admisión dinámica compatible con la topología. Esta característica es clave para solucionar "la undécima sesión" descrita anteriormente. La señalización RSVP envía un mensaje relativo a los recursos necesarios a dispositivos en la ruta de los datos. Por tanto, los dispositivos compatibles con RSVP son capaces de evaluar de forma dinámica las repercusiones que tendría el tráfico de datos asociados en los recursos y de notificar a los dispositivos ascendentes cuando no tienen los recursos necesarios para controlar los flujos de tráfico adicionales. En el caso de la "undécima sesión de telefonía", los dispositivos de red rechazarán la admisión del decimoprimero flujo de tráfico en la cola de baja latencia. De esta forma, se protegen las diez sesiones existentes. Es importante darse cuenta de que la señalización basada en host no impide el control del administrador de la red sobre los recursos de red. Simplemente ofrece información a la red que se puede utilizar para facilitar la administración de los recursos de red.

5.3.3.3. Calidades de las garantías y el producto de calidad/eficacia

El tráfico telefónico se caracteriza por la necesidad de garantías de alta calidad. Tiene requisitos cuantificables y su valor depende de que estos requisitos se cumplan con precisión. Las aplicaciones multimedia suelen requerir garantías de alta calidad. No todas las aplicaciones requieren garantía de alta calidad. Por ejemplo, las transacciones de bases de datos de cliente/servidor, no pueden cuantificar de forma precisa los requisitos de recursos y, por tanto, no exigen garantías cuantificables. Estas aplicaciones se

pueden beneficiar de garantías de calidad menor que pueden reducir la latencia pero es posible que no ofrezcan un límite preciso de latencia.

Una forma de proporcionar garantías de alta calidad es proveer considerablemente la red. Por ejemplo, si los dispositivos de red descritos en el ejemplo de la telefonía IP hubieran sido provistos para ser compatibles con todas las posibles sesiones de telefonía IP, se podría haber evitado el problema de la "undécima sesión". Sin embargo, si hay mil posibles sesiones pero, en término medio, sólo diez sesiones simultáneas, sería necesario proveer en exceso los dispositivos de red por un factor de cien con el objetivo de permitir garantías de alta calidad. Se trata evidentemente de un uso ineficaz de los recursos de red. Existe un intercambio entre la capacidad de una red para ofrecer las garantías de alta calidad y la eficacia con la que se pueden utilizar los recursos de red. Una red se puede caracterizar mediante un producto de calidad/eficacia (producto QE) constante. Ofrecer garantías de alta calidad exige un compromiso de eficacia y viceversa.

Un mecanismo alternativo para proporcionar garantías de alta calidad es la utilización de la señalización RSVP, tal como se ha descrito anteriormente. Con este tipo de señalización, se pueden proveer los dispositivos de red para la carga media esperada. En la excepcional ocasión en la que la carga sobrepasa las expectativas, se rechazarán sesiones adicionales, pero se mantendrá la integridad de las garantías ofrecidas en sesiones existentes. Al utilizar la señalización RSVP, se puede incrementar el producto QE de la red, y al mismo tiempo ofrecer garantías de alta calidad y utilizar los recursos de red de forma más eficaz. Cuanto más sofisticado sea un mecanismo de QoS, más posibilidades habrá de incrementar el producto QE de una red en particular. Podría parecer que todos los dispositivos de red deberían implementar los mecanismos más sofisticados de QoS disponibles. Sin embargo, los mecanismos de QoS tienen un elevado coste relacionado con la compatibilidad misma del mecanismo de QoS. En el caso de la señalización, este exceso adopta la forma

de recursos de procesamiento en dispositivos de red. Este hecho nos lleva a un aspecto muy importante: debería evaluarse cualquier mecanismo de QoS en términos de la ventaja que ofrece en función del producto QE incrementado frente al coste que conlleva en términos de exceso incrementado.

La siguiente tabla ilustra esta concepción en términos de mecanismos de QoS reales:

Tabla 9: Mecanismos de QoS

	Aprovisionamiento de arriba abajo	**Aprovisionamiento de arriba abajo**	**Señalización por conversación**
Sin tratamiento de tráfico	Cola FIFO	Control de admisión de agregados	Control de admisión por conversación
Tratamiento de tráfico agregado	diffserv/802.1p aprovisionado de arriba abajo	RSVP/diffserv agregado RSVP/802.1p agregado	RSVP/diffserv RSVP/802.1p
Tratamiento de tráfico por conversación			RSVP/Intserv

Producto QE mejorado (mayor sobrecarga)

Las líneas de la tabla 8 corresponden a los niveles incrementados de sofisticación en los mecanismos de control del tráfico. Las columnas corresponden a los niveles de sofisticación incrementados en los mecanismos de provisión y configuración. Observe la celda superior izquierda, que no representa ningún mecanismo de QoS y que ofrece un producto QE limitado. Una LAN provista en exceso es un ejemplo de una red de este tipo. En el extremo contrario, observe la celda inferior derecha, que representa una red en la que cada elemento de red procesa la señalización RSVP por conversación y aplica el control del tráfico intserv por conversación. Las celdas intermedias representan compromisos entre producto QE incrementado y nivel de exceso. La celda que representa la combinación del control de admisión por

conversación y el control de tráfico por acumulación resulta de especial interés.

5.3.3.4. QoS en la red de la Universidad Don Bosco

Como se ha visto hasta el momento, existen diversos mecanismos para controlar el tráfico de una red, así como aprovisionarlo y configurarlo. Estos mecanismos son muchas veces complicados y a veces hasta costosos para los administradores de dichas redes. Hay que agregar que actualmente los anchos de banda son relativamente baratos por lo que en la mayoría de casos se opta por sobredimensionar los enlaces adecuadamente para evitar el congestionamiento. Probablemente esto cambie con las futuras aplicaciones de Ethernet de 10 Gigabits en redes metropolitanas o de área extensa, donde el aumento de capacidad puede tener unos costos mayores.

Como se observó en la tabla 8, el modelo más adecuado para tener recursos reservados entre los extremos de la red es el RSVP/Intserv. Curiosamente a pesar del interés que el modelo IntServ suscitó entre la comunidad Internet su uso no se ha difundido, ni entre los fabricantes que han sido reacios a implementarlo en los equipos, ni entre los ISPs, que tampoco lo han desarrollado en sus redes. Según los expertos, el fracaso del modelo IntServ se debe a su no escalabilidad, es decir a que el costo de su implementación crece cuando menos linealmente con la complejidad de la red. El problema está en que, al ser RSVP un protocolo orientado a conexión los routers han de mantener una información de estado de todos los flujos activos que pasan por ellos. Esta información de estado puede ser aceptable en los routers de la periferia, pero resulta inmanejable en los routers centrales de la red que han de soportar miles de conexiones activas.

Como alternativa se tiene el modelo de prioritización Diffserv. La idea básica de DiffServ consiste en que cada paquete lleva escrito un código que indica a que clase pertenece; se supone que los routers saben el tratamiento que han de dar a cada una de las clases posibles, por lo que no han de mantener ninguna información sobre conexiones o flujos concretos; el número de clases posibles es limitado e independiente del número de hosts o de flujos que pasan por los routers, por lo que la arquitectura DiffServ es escalable. De hecho, este modelo utiliza a su manera los campos ToS en Ipv4 y el Traffic Class del Ipv6.

Para concluir, es necesario evaluar la necesidad de la red avanzada en la Universidad Don Bosco, para esto se recomienda analizar por medio de la medición parámetros como la perdida de paquetes, el retardo y el jitter. Para esto se recomienda diseñar un modelo, que tome en cuenta estos parámetros, los tiempos de respuesta y además que proporcione la disponibilidad de la red. Este modelo servirá para poder evaluar cual modelo de QoS es el más adecuado implementar en la red avanzada de la Universidad Don Bosco y de ser factible, ampliarlo para su utilización dentro de la red Internet.

5.4. PROTOCOLO PARA VIDEOCONFERENCIA H.323

El estándar H.323 proporciona una base para las comunicaciones de audio, video y datos a través de una red IP como Internet. Los productos que cumplen con el estándar H.323 pueden ínter operar con los productos de otros, permitiendo de esta manera que los usuarios puedan comunicarse sin preocuparse con problemas de compatibilidad.

H.323 es un estándar bajo el amparo de la ITU; es un conjunto de estándares para la comunicación multimedia sobre redes que no proporcionan calidad de servicio (QoS). Estas redes son las que predominan hoy en todos los lugares, como redes de paquetes conmutadas TCP/IP e IP sobre Ethernet, Fast

Ethernet y Token Ring. Por esto, los estándares H.323 son bloques importantes de construcción para un amplio rango de aplicaciones basadas en redes de paquetes para la comunicación multimedia y el trabajo colaborativo.

El estándar tiene amplitud e incluye desde dispositivos específicos hasta tecnologías embebidas en computadoras personales, además de servir para comunicación punto-punto o conferencias multi-punto. H.323 habla también sobre control de llamadas, gestión multimedia y gestión de ancho de banda, además de las interfases entre redes de paquetes y otras redes. H.323 forma parte de una gran serie de estándares que permiten la videoconferencia a través de redes. Conocidos como H.32X, esta serie incluye H.320 y H.324, que permiten las comunicaciones RDSI y RTC respectivamente.

5.4.1. Arquitectura

H.323 cubre los requerimientos técnicos para los servicios de comunicaciones entre Redes Basadas en Paquetes (PBN) que pueden no proporcionar calidad de servicio (QoS). Estas redes de paquetes pueden incluir Redes de Área Local (LAN's), Redes de Área Extensa (WAN), Intra-Networks e Inter-Networks (incluyendo Internet). También incluye conexiones telefónicas o punto a punto sobre RTC o ISDN que usan debajo un transporte basado en paquetes como PPP. Esas redes pueden consistir de un segmento de red sencillo, o pueden tener topologías complejas que pueden incorporar muchos segmentos de red interconectados por otros enlaces de comunicación.

El estándar describe los componentes de un sistema H.323, estos son: Terminales, Gateways, Gatekeepers, y Unidades de Control Multipunto (MCU).

5.4.1.1. Terminales

Los terminales son puntos finales de la comunicación. Proporcionan comunicación en tiempo real bidireccional. Para permitir que cualesquiera terminales ínter operen se define que todos deben tener un mínimo denominador que es, soportar voz y con un códec G.711. De esta manera el soporte para video y datos es opcional para un terminal H.323.

Todos los terminales deben soportar H.245, el cual es usado para negociar el uso del canal y las capacidades. Otros tres componentes requeridos son: Q.931 para señalización de llamada y configuración de llamada, un componente llamado RAS (Registration/Admision/Status), este es un protocolo usado para comunicar con el Gatekeeper; y soporte para RTP/RTCP para secuenciar paquetes de audio y video.

Otros componentes opcionales de los terminales H.323 son: los códec de video, los protocolos T.120 para datos y las capacidades MCU.

5.4.1.2. Gateways

El Gateway (o Pasarela) es un elemento opcional de una conferencia H.323. Es necesario solo si necesitamos comunicar con un terminal que está en otra red (por ejemplo RTC). Los Gateways proporcionan muchos servicios, el más común es la traducción entre formatos de transmisión (por ejemplo H.225.0 a H.221) y entre procedimientos de comunicación (por ejemplo H.245 a H.242). Además el Gateway también traduce entre los códecs de video y audio usados en ambas redes y procesa la configuración de la llamada y limpieza de ambos lados de la comunicación.

El Gateway es un tipo particular de terminal y es una entidad “llamable” (tiene una dirección).

En general, el propósito del Gateway es reflejar las características del terminal en la Red de Circuitos Conmutados (SCN) y al contrario. Las principales aplicaciones de los Gateways son:

- Establecer enlaces con terminales telefónicos analógicos conectados a la RTB (Red Telefónica Básica).
- Establecer enlaces con terminales remotos que cumple H.320 sobre redes RDSI basadas en circuitos conmutados (SCN).
- Establecer enlaces con terminales remotos que cumple H.324 sobre red telefónica básica (RTB).

Los Gateways no se necesitan si las conexiones son entre redes basadas en paquetes.

Muchas funciones del Gateway son dejadas al diseñador. Por ejemplo, el número de terminales H.323 que pueden comunicar a través del Gateway no es asunto de estandarización. De la misma manera el número de conexiones con la SCN, el número de conferencias individuales soportadas, las funciones de conversión de audio/video/datos, y la inclusión de funciones multipuntos son dejadas al diseñador. Debido a la incorporación de los Gateways a la especificación H.323, la ITU posicionó H.323 como el pegamento que junta todos los terminales para conferencias funcionando al mismo tiempo.

5.4.1.3. Gatekeepers

Son un elemento opcional en la comunicación entre terminales H.323. No obstante, son el elemento más importante de una red H.323. Actúan como punto central de todas las llamadas dentro de una zona y proporcionan servicios a los terminales registrados y control de las llamadas. De alguna forma, el gatekeeper H.323 actúa como un conmutador virtual.

Los Gatekeepers proporcionan dos importantes funciones de control de llamada:

- Traducción de direcciones desde alias de la red H.323 a direcciones IP o IPX, tal y como está especificado en RAS.
- Gestión de ancho de banda, también especificado en RAS. Por ejemplo, si un administrador de red ha especificado un umbral para el número de conferencias simultáneas, el Gatekeeper puede rechazar hacer más conexiones cuando se ha alcanzado dicho umbral. El efecto es limitar el ancho de banda total de las conferencias a alguna fracción del total existente para permitir que la capacidad remanente se use para e-mail, transferencias de archivos y otros protocolos.

A la colección de todos los Terminales, Gateways y MCU's gestionados por un gatekeeper se la conoce como Zona H.323.

Una característica opcional, pero valiosa de los gatekeepers es la habilidad para enrutar llamadas. Si se enruta la llamada por un gatekeeper, esta puede ser controlada más efectivamente. Los proveedores de servicio necesitan esta característica para facturar por las llamadas realizadas a través de su red. Este servicio también puede ser usado para re-enrutar una llamada a otro terminal en caso de estar no disponible el llamado. Además con esta característica un gatekeeper puede tomar decisiones que involucren el balanceo entre varios gateways. Por ejemplo, si una llamada es enrutada por un gatekeeper, ese gatekeeper puede re-enrutar la llamada a uno de varios gateways basándose en alguna lógica de enrutamiento propietaria.

Mientras que un Gatekeeper está lógicamente separado de los extremos de una conferencia H.323, los fabricantes pueden elegir incorporar la funcionalidad del Gatekeeper dentro de la implementación física de Gateways y MCU's.

A pesar de que el Gatekeeper no es un elemento obligatorio, si existe, los terminales deben usarlo. RAS define para estos la traducción de direcciones, control de admisión, control de ancho de banda y gestión de zonas.

Los Gatekeepers juegan también un rol en las conexiones multipunto. Para soportar conferencias multipunto, los usuarios podrían emplear un Gatekeeper para recibir los canales de control H.245 desde dos terminales en una conferencia punto-punto. Cuando la conferencia cambia a multipunto, el Gatekeeper puede redireccionar el Canal de Control H.245 a un controlador multipunto, el MC. El Gatekeeper no necesita procesar la señalización H.245, solo necesita pasarla entre los terminales o entre los terminales y el MC.

Las redes que posean un Gateway pueden también tener un Gatekeeper para traducir llamadas entrantes E.164 (número de teléfono convencional) a direcciones de transporte. Debido a que una Zona está definida por su Gatekeeper, las entidad H.323 que contengan un Gatekeeper interno necesitan de un mecanismo para desactivar su funcionamiento cuando hay varias entidades H.323 que contienen un Gatekeeper dentro de la red, las entidades pueden ser configuradas para estar en la misma Zona.

Existen dos formas para que un terminal se registre en un gatekeeper, sabiendo su IP y enviando entonces un mensaje de registro unicast a esta dirección o bien enviando un mensaje multicast de descubrimiento del gatekeeper (GRQ) que pregunta ¿quién es mi gatekeeper?

Funciones obligatorias Gatekeeper

- Traducción de Direcciones: Traducción de alias a direcciones de transporte, usando para ello una tabla que es modificada con mensajes

de Registro (Registration). Se permiten otros métodos de modificar la tabla.

- Control de Admisión: El Gatekeeper debería autorizar el acceso a la red usando mensajes H.225.0 ARQ/ACF/ARJ. Esto puede basarse en autorización de llamada, ancho de banda, o algún otro criterio que es dejado al fabricante. También puede ser una función nula que admita todas las peticiones.
- Control de Ancho de Banda: El Gatekeeper debería soportar mensajes BRQ/BRJ/BCF. Esto puede usarse para gestión del ancho de banda. También se puede aceptar todas las peticiones de ancho de banda.
- Gestión de Zona: El Gatekeeper debería suministrar la funciones anteriores a: todos los terminales, MCU's y Gateways que se encuentren registrados en su Zona de control.

Funciones opcionales Gatekeeper

- Señalización de control de llamada: El Gatekeeper puede elegir completar la señalización de llamada con los extremos y procesar la señalización de llamada él mismo. Alternativamente, puede elegir que los extremos conecten directamente sus señalizaciones de llamada. De esta manera el Gatekeeper puede evitar gestionar las señales de control H.225.0.
- Autorización de llamada: El Gatekeeper puede rechazar una llamada desde un terminal basándose en la especificación Q.931 (H.225.0). Las razones para rechazar la llamada pueden ser, pero no están limitadas a, acceso restringido desde o hacia un terminal particular o Gateway, y acceso restringido durante un periodo de tiempo. El criterio para determinar si se pasa la autorización o falla, está fuera del alcance de H.323.
- Gestión de llamada: El Gatekeeper puede mantener una lista de las llamadas en curso, esta información puede ser usada para indicar si un

terminal está ocupado o para dar información a la función de gestión de ancho de banda.

- Otros como: estructura de datos de información para la gestión, reserva de ancho de banda y servicios de directorio.

5.4.1.4. Unidades Control Multipunto (MCU)

La MCU soporta conferencias entre tres o más extremos. En terminología H.323, el MCU se compone de: Controlador Multipunto (MC) que es obligatorio, y cero o más Procesadores Multipunto (MP). El MC gestiona las negociaciones H.245 entre todos los terminales para determinar las capacidades comunes para el procesado de audio y video. El MC también controla los recursos de la conferencia para determinar cuales de los flujos, si hay alguno, serán multicast. Las capacidades son enviadas por el MC a todos los extremos en la conferencia indicando los modos en los que pueden transmitir. El conjunto de capacidades puede variar como resultado de la incorporación o salida de terminales de la conferencia.

El MC no trata directamente con ningún flujo de datos, audio o video. Esto se lo deja al MP, este mezcla, conmuta y procesa audio, video y/o bits de datos. Las capacidades del MC y MP pueden estar implementadas en un componente dedicado o ser parte de otros componentes H.323, en concreto puede ser parte de un Gatekeeper, un Gateway, un terminal o una MCU.

El MP recibe flujos de audio, video o datos desde los extremos, estos pueden estar involucrados en una conferencia centralizada, descentralizada o híbrida. El MP procesa esos flujos y los devuelve a los extremos.

5.5. PROTOCOLO DE INTERNET IPv6

IPv6 es la versión 6 del Protocolo de Internet (Internet Protocol), un estándar del nivel de red encargado de dirigir y encaminar los paquetes a través de una red.

Diseñado por Steve Deering de Xerox PARC y Craig Mudge, IPv6 está destinado a sustituir al estándar IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados. Pero el nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionando a futuras celdas telefónicas y dispositivos móviles con sus direcciones propias y permanentes. Al día de hoy se calcula que las dos terceras partes de las direcciones que ofrece IPv4 ya están asignadas.

IPv4 soporta 4,294,967,296 (2^{32}) direcciones de red diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos para cada coche, teléfono, PDA o tostadora; mientras que IPv6 soporta 340,282,366,920,938,463,463,374,607,431,768,211,456 (2^{128} ó 340 sextillones) de direcciones; cerca de 4.3×10^{20} (430 trillones) de direcciones por cada pulgada cuadrada ($6,7 \times 10^{17}$ ó 670 mil billones direcciones/mm^2) de la superficie de La Tierra.

La adopción de IPv6 ha sido frenada por la traducción de direcciones de red (NAT), que alivia parcialmente el problema de la falta de direcciones IP. Pero NAT hace difícil o imposible el uso de algunas aplicaciones P2P, como son la voz sobre IP (VoIP) y juegos multiusuario. Además, NAT rompe con la idea originaria de Internet donde todos pueden conectarse con todos. Actualmente, el gran catalizador de IPv6 es la capacidad de ofrecer nuevos servicios, como la movilidad, Calidad de Servicio (QoS), privacidad, etc. El gobierno de los Estados Unidos ha ordenado el despliegue de IPv6 por todas sus agencias federales para el año 2008.

5.5.1. Características de IPv6

A continuación se enumeran las características del nuevo protocolo IPv6:

- Nuevo formato de encabezado
- Gran espacio de direcciones
- Direccionamiento jerárquico e infraestructura de enrutamiento eficientes
- Configuración de direcciones sin estado y con estado
- Seguridad integrada
- Mayor compatibilidad con QoS
- Nuevo protocolo para la interacción de nodos vecinos
- Capacidad de ampliación

Nuevo formato de encabezado

El encabezado de IPv6 presenta un nuevo formato diseñado para que la carga de trabajo del encabezado sea mínima. Para ello, se mueven los campos de opciones y los que no son esenciales a encabezados de extensión que se colocan tras el encabezado de IPv6. El encabezado optimizado de IPv6 proporciona un procesamiento más eficiente en los routers intermedios.

Los encabezados de IPv4 no pueden funcionar conjuntamente con los encabezados de IPv6. Un host o un router deben utilizar una implementación de IPv4 e IPv6 para reconocer y procesar ambos formatos de encabezado. El nuevo encabezado de IPv6 es sólo el doble de grande que el de IPv4, aunque las direcciones de IPv6 son cuatro veces mayores que las de IPv4.

Gran espacio de direcciones

IPv6 tiene direcciones IP de origen y destino de 128 bits (16 bytes). Aunque con 128 bits se pueden expresar más de $3.4x10^{38}$ combinaciones posibles, el gran espacio de direcciones de IPv6 se ha diseñado para permitir

varios niveles de subredes y asignaciones de redes de la red troncal de Internet a las subredes individuales de una organización.

Aunque actualmente sólo se asigna un pequeño número de las direcciones posibles para los hosts, hay muchas direcciones disponibles para su uso en el futuro. Con un número de direcciones disponibles mucho mayor, dejan de ser necesarias las técnicas de conservación de direcciones, como la distribución de NAT.

Direccionamiento jerárquico e infraestructura de enrutamiento eficientes

Las direcciones globales de IPv6 utilizadas en la parte IPv6 de Internet están diseñadas para crear una infraestructura de enrutamiento jerárquica eficiente que se puede resumir, basada en la aparición de múltiples niveles de proveedores de servicios de Internet. En Internet IPv6, los router troncales tienen tablas de enrutamiento mucho más pequeñas, que corresponden a la infraestructura de enrutamiento de Agregadores de nivel superior.

Configuración de direcciones sin estado y con estado

Para simplificar la configuración de hosts, IPv6 permite la configuración de direcciones con estado, como la configuración de direcciones en presencia de un servidor DHCP, y la configuración de direcciones sin estado (configuración de direcciones en ausencia de un servidor DHCP). Con una configuración de direcciones sin estado, los hosts de un vínculo se configuran automáticamente con direcciones IPv6 para el vínculo (que se denominan direcciones locales de vínculo) y con direcciones derivadas de prefijos anunciados por routers locales. Incluso en ausencia de un router, los hosts del mismo vínculo pueden configurarse automáticamente con direcciones locales de vínculo y se comunican sin configuración manual.

Seguridad integrada

La compatibilidad con IPSec es un requisito del conjunto de protocolos IPv6. Este requisito proporciona una solución basada en estándares en respuesta a las necesidades de seguridad de red y aumenta la interoperabilidad entre distintas implementaciones de IPv6.

Mayor compatibilidad con QoS

Los nuevos campos del encabezado de IPv6 definen cómo se identifica y se controla el tráfico. La identificación del tráfico mediante un campo Flow Label (Etiqueta de flujo) en el encabezado de IPv6 permite a los routers identificar y proporcionar un tratamiento especial a los paquetes que pertenecen a un flujo, un conjunto de paquetes que viaja entre un origen y un destino. Como el tráfico se identifica en el encabezado de IPv6, se puede proporcionar compatibilidad con QoS incluso si la carga de paquetes está cifrada mediante IPSec.

Nuevo protocolo para la interacción de nodos vecinos

El protocolo Neighbor Discovery (Descubrimiento de vecino) para IPv6 consiste en un conjunto de mensajes del Protocolo de mensajes de control de Internet para IPv6 (ICMPv6, Internet Control Message Protocol for IPv6) que administran la interacción de nodos vecinos (nodos que se encuentran en el mismo vínculo). Neighbor Discovery reemplaza al Protocolo de resolución de direcciones (ARP, Address Resolution Protocol) basado en difusión, al protocolo de descubrimiento de enrutadores de ICMPv4 y a los mensajes Redirect (Redirección) de ICMPv4 con mensajes Neighbor Discovery de unicast y multicast.

Capacidad de ampliación

IPv6 se puede ampliar fácilmente con nuevas características si se agregan encabezados de extensión tras el encabezado de IPv6. A diferencia de las opciones del encabezado de IPv4, que sólo permite 40 bytes de opciones, el

tamaño de los encabezados de extensión de IPv6 sólo está limitado por el tamaño del paquete de IPv6.

5.5.2. Diferencias entre IPv4 e IPv6

En la tabla 9 se resaltan algunas de las principales diferencias entre IPv4 e IPv6.

Tabla 10: Diferencias entre IPv4 e IPv6

IPv4	**IPv6**
Las direcciones de origen y de destino tienen una longitud de 32 bits (4 bytes).	Las direcciones de origen y de destino tienen una longitud de 128 bits (16 bytes).
La compatibilidad con IPSec es opcional.	La compatibilidad con IPSec es obligatoria.
No hay identificación de carga para el control de QoS por parte de los routers en el encabezado de IPv4.	La identificación de carga para el control de QoS por parte de los routers se incluye en el encabezado de IPv6 mediante el campo Flow Label (Etiqueta de flujo).
La fragmentación es posible en ambos routers y en el host de envío.	La fragmentación no es posible en los routers. Sólo es posible en el host de envío.
El encabezado incluye una suma de comprobación.	El encabezado no incluye una suma de comprobación.
El encabezado incluye opciones.	Todos los datos opcionales se mueven a extensiones de encabezado IPv6.
El Protocolo de resolución de direcciones (ARP) utiliza tramas de solicitud de ARP de difusión para resolver una dirección de IPv4 en una dirección de nivel de vínculo.	Las tramas de solicitud de ARP se reemplazan por mensajes Neighbor Solicitation (Solicitud de vecino) de multicast.
Se utiliza el Protocolo de administración de grupos de Internet (IGMP) para administrar la pertenencia a grupos de subredes locales.	El protocolo IGMP se reemplaza por mensajes Multicast Listener Discovery (MLD o Descubrimiento de escucha de multicast).
Para determinar la dirección IPv4 de la mejor puerta de enlace predeterminada	El descubrimiento de routers de ICMPv4 se reemplaza por los mensajes Router

se utiliza el descubrimiento de routers de ICMP, que es opcional.	Solicitation (Solicitud de router) y Router Advertisement (Anuncio de router) de ICMPv6, que son necesarios.
Las direcciones de difusión se utilizan para enviar tráfico a todos los nodos de una subred.	No hay direcciones de difusión de IPv6. En su lugar, se utiliza una dirección de multicast para todos los nodos de ámbito local de vínculo.
La configuración debe efectuarse manualmente o a través de DHCP.	No se necesita configuración manual ni DHCP.
Utiliza registros de recursos (A) de dirección de host en el Sistema de nombres de dominio (DNS, Domain Name System) para asignar nombres de host a direcciones IPv4.	Utiliza registros de recursos (AAAA) de dirección de host en el Sistema de nombres de dominio (DNS) para asignar nombres de host a direcciones IPv6.
Utiliza registros del recurso Puntero (PTR) en el dominio DNS IN-ADDR.ARPA para asignar direcciones de IPv4 a nombres de host.	Utiliza registros del recurso Puntero (PTR) en el dominio DNS IP6.INT para asignar direcciones de IPv6 a nombres de host.

5.5.3. Direccionamiento IPv6

El cambio más drástico de IPv4 a IPv6 es la longitud de las direcciones de red. Las direcciones IPv6, definidas en el RFC 2373 y RFC 2374, son de 128 bits; esto corresponde a 32 dígitos hexadecimales, que se utilizan normalmente para escribir las direcciones IPv6, como se describe más adelante.

El número de direcciones IPv6 posibles es de $2^{128} \approx 3.4 \times 10^{38}$. Este número puede también representarse como 16^{32}, con 32 dígitos hexadecimales, cada uno de los cuales puede tomar 16 valores.

En muchas ocasiones las direcciones IPv6 están compuestas por dos partes lógicas: un prefijo de 64 bits y otra parte de 64 bits que corresponde al

identificador de interfaz, que casi siempre se genera automáticamente a partir de la dirección MAC de la interfaz a la que está asignada la dirección.

5.5.3.1. Notación para las direcciones IPv6

Las direcciones IPv6, de 128 bits de longitud, se escriben como ocho grupos de cuatro dígitos hexadecimales.

Por ejemplo,

2001:0db8:85a3:08d3:1319:8a2e:0370:7334

Es una dirección IPv6 válida.

Si un grupo de cuatro dígitos es nulo (es decir, toma el valor "0000"), puede ser comprimido. Por ejemplo,

2001:0db8:85a3:0000:1319:8a2e:0370:7344

Es la misma dirección que

2001:0db8:85a3::1319:8a2e:0370:7344

Siguiendo esta regla, si más de dos grupos consecutivos son nulos, pueden comprimirse como "::". Si la dirección tiene más de una serie de grupos nulos consecutivos la compresión solo en uno de ellos. Así:

2001:0DB8:0000:0000:0000:0000:1428:57ab
2001:0DB8:0000:0000:0000::1428:57ab
2001:0DB8:0:0:0:0:1428:57ab
2001:0DB8:0::0:1428:57ab
2001:0DB8::1428:57ab

Son todas válidas y significan lo mismo, pero

2001::25de::cade

Es inválido porque no queda claro cuantos grupos nulos hay en cada lado.

Los ceros iniciales en un grupo pueden ser omitidos. Así:

2001:0DB8:02de::0e13

Es lo mismo que

2001:DB8:2de::e13

Si la dirección es una dirección IPv4 camuflada, los últimos 32 bits pueden escribirse en base decimal; así:

::ffff:192.168.89.9 es lo mismo que
::ffff:c0a8:5909, pero no lo mismo que
::192.168.89.9 ó
::c0a8:5909.

El formato :ffff:1.2.3.4 se denomina dirección IPv4 mapeada, y el formato ::1.2.3.4 dirección IPv4 compatible.

Las direcciones IPv4 pueden ser transformadas fácilmente al formato IPv6. Por ejemplo, si la dirección decimal IPv4 es 135.75.43.52 (en hexadecimal, 0x874B2B34), puede ser convertida a 0000:0000:0000:0000:0000:0000:874B:2B34 ó ::874B:2B34. Entonces, uno puede usar la notación mixta dirección IPv4 compatible, en cuyo caso la dirección debería ser ::135.75.43.52. Este tipo de dirección IPv4 compatible casi no está siendo utilizada en la práctica, aunque los estándares no la han declarado obsoleta.

5.5.3.2. Identificación de los tipos de direcciones

Los tipos de direcciones IPv6 pueden identificarse tomando en cuenta los primeros bits de cada dirección.

- ::/128 – la dirección con todo ceros se utiliza para indicar la ausencia de dirección, y no se asigna ningún nodo.
- ::1/128 – la dirección de loopback es una dirección que puede usar un nodo para enviarse paquetes a sí mismo (corresponde con 127.0.0.1 de IPv4). No puede asignarse a ninguna interfaz física.
- ::/96 – La dirección IPv4 compatible se usa como un mecanismo de transición en las redes duales IPv4/IPv6.
- ::ffff:0:0/96 – La dirección IPv4 mapeada es usada como un mecanismo de transición en terminales duales.
- fe80::/10 – El prefijo de enlace local (local link) específica que la dirección sólo es válida en el enlace físico local.
- fec0::/10 – El prefijo de emplazamiento local (site-local prefix) específica que la dirección sólo es válida dentro de una organización local. La RFC3879 lo declaró obsoleto, estableciendo que los sistemas futuros no deben implementar ningún soporte para este tipo de dirección especial.
- ff00::/8 – El prefijo de multicast es usado para las direcciones multicast.

Hay que resaltar que las direcciones de difusión (broadcast) no existen en IPv6, aunque la funcionalidad que prestan puede emularse utilizando la dirección multicast FF01::1, denominada todos los nodos (all nodes).

5.5.4. Paquetes IPv6

Un paquete en IPv6 está compuesto principalmente de dos partes: la cabecera y los datos.

La cabecera está en los primeros 40 bytes del paquete y contiene las direcciones de origen y destino (128 bits cada una), la versión de IP (4 bits), la

clase de tráfico (8 bits, Prioridad del Paquete), etiqueta de flujo (20 bits, manejo de la Calidad de Servicio), longitud de carga (16 bits, longitud del campo de datos), siguiente encabezado (8 bits), y límite de saltos (8 bits, Tiempo de Vida). Después viene el campo de datos, con los datos que transporta el paquete, que puede llegar a 64k de tamaño en el modo normal, o más con la opción "jumbo payload".

Figura 19: Encabezado de IPv6.

A continuación se describen más a detalle:

Version (Versión): se utilizan 4 bits para indicar la versión de IP, que se establece en el valor 6.

Traffic Class (Clase de tráfico): indica la clase o la prioridad del paquete IPv6. El tamaño de este campo es de 8 bits. El campo Traffic Class proporciona una funcionalidad similar a la del campo Type of Service (Tipo de servicio) de IPv4. En RFC 2460, no están definidos los valores del campo Traffic Class. Sin embargo, se necesita una implementación de IPv6 para proporcionar un medio que permita a un protocolo de nivel de aplicación especificar el valor del campo Traffic Class para experimentación.

Flow Label (Etiqueta de flujo): indica que este paquete pertenece a una secuencia específica de paquetes entre un origen y un destino, lo que requiere

un control especial por parte de los routers IPv6 intermedios. El tamaño de este campo es de 20 bits. El campo Flow Label se utiliza para conexiones de calidad de servicio que no son predeterminadas, como las que se necesitan para los datos en tiempo real (voz y vídeo). Para el control del router predeterminado, el campo Flow Label se establece en el valor 0. Puede haber varios flujos entre un origen y un destino, lo que se distingue mediante etiquetas de flujo independientes con un valor distinto de cero.

Payload Length (Longitud de carga): indica la longitud de la carga IP. El tamaño de este campo es de 16 bits. El campo Payload Length incluye los encabezados de extensión y la unidad PDU de nivel superior. Con 16 bits, se puede indicar una carga IPv6 de hasta 65.535 bytes. Para longitudes de carga superiores a 65.535 bytes, el campo Payload Length se establece en el valor 0 y se utiliza la opción de carga Jumbo en el encabezado de extensión Hop-by-Hop Options (Opciones de salto a salto).

Next Header (Encabezado siguiente): indica el primer encabezado de extensión (si existe) o el protocolo de la unidad PDU de nivel superior (como TCP, UDP o ICMPv6). El tamaño de este campo es de 8 bits. Cuando se indica un protocolo de nivel superior por encima de la capa de Internet, se utilizan aquí los mismos valores que en el campo Protocol (Protocolo) de IPv4.

Hop Limit (Límite de saltos): indica el número máximo de vínculos por los que puede viajar el paquete IPv6 antes de que se descarte. El tamaño de este campo es de 8 bits. El campo Hop Limit es similar al campo TTL de IPv4, excepto en que no existe ninguna relación histórica en cuanto al tiempo (en segundos) que el paquete está en cola en el router. Cuando el límite de saltos es igual a 0, el paquete se descarta y se envía un mensaje Time Expired (Fin de tiempo de espera) de ICMP a la dirección IP de origen.

Source Address (Dirección de origen): almacena la dirección IPv6 del host de origen. El tamaño de este campo es de 128 bits.

Destination Address (Dirección de destino): almacena la dirección IPv6 del host de destino actual. El tamaño de este campo es de 128 bits. En la mayoría de los casos, la dirección de destino se establece en la dirección de destino final. Sin embargo, si hay un encabezado de extensión de enrutamiento, la dirección de destino se puede establecer en la interfaz del siguiente router de la lista de rutas de origen.

Hay dos versiones de IPv6 levemente diferentes. La ahora obsoleta versión inicial, descrita en el RFC1883, difiere de la actual versión estándar, descrita en el RFC2460, en dos campos: 4 bits han sido reasignados desde "etiqueta de flujo" (flow label) a "clase de tráfico" (traffic class). El resto de diferencias son menores.

En IPv6 la fragmentación se realiza sólo en el nodo origen del paquete, al contrario que en IPv4 en donde los routers pueden fragmentar un paquete. En IPv6, las opciones también se salen de la cabecera estándar y son especificadas por el campo "Cabecera Siguiente" (Next Header), similar en funcionalidad en IPv4 al campo Protocolo. Un ejemplo: en IPv4 uno añadiría la opción "ruta fijada desde origen" (Strict Source and Record Routing) a la cabecera IPv4 si quiere forzar una cierta ruta para el paquete, pero en IPv6 uno modificaría el campo "Cabecera Siguiente" indicando que una cabecera de encaminamiento es la siguiente en venir. La cabecera de encaminamiento podrá entonces especificar la información adicional de encaminamiento para el paquete, e indicar que, por ejemplo, la cabecera TCP será la siguiente. Este procedimiento es análogo al de AH y ESP en IPsec para IPv4 (que aplica a IPv6 de igual modo, por supuesto).

Configuración automática de direcciones

Uno de los aspectos más útiles de IPv6 es su capacidad para configurarse automáticamente, incluso sin ayuda de un protocolo de configuración con estado como el Protocolo de configuración dinámica de host para IPv6 (DHCPv6). De forma predeterminada, un host IPv6 puede configurar una dirección local de vínculo para cada interfaz. Mediante el proceso de descubrimiento de routers, un host también puede determinar las direcciones de los routers, otros parámetros de configuración, direcciones adicionales y prefijos en el vínculo. En el mensaje Router Advertisement (Anuncio de router) incluye una indicación de si debe utilizarse un protocolo de configuración de direcciones con estado.

La configuración automática de direcciones sólo se puede llevar a cabo con interfaces compatibles con multicast. La configuración automática de direcciones se describe en RFC2462.

Con excepción de una configuración automática para direcciones locales de vínculo, la configuración automática de direcciones sólo se especifica para los hosts. Los routers deben obtener los parámetros de configuración y de dirección por otros medios, tales como la configuración manual.

Despliegue de IPv6

El 20 de julio de 2004 la Corporación de Internet para la Asignación de Nombres y Números (ICANN, Internet Corporation for Assigned Names and Numbers) anunció que los servidores raíz de DNS de Internet habían sido modificados para soportar ambos protocolos, IPv4 e IPv6.

Desventajas:

- La necesidad de extender un soporte permanente para IPv6 a través de todo Internet y de los dispositivos conectados a ella.
- Para estar enlazada al universo IPv4 durante la fase de transición, todavía se necesita una dirección IPv4 o algún tipo de NAT (compartición

de direcciones IP) en los routers pasarela (IPv6<-->IPv4) que añaden complejidad y que significa que el gran espacio de direcciones prometido por la especificación no podrá ser inmediatamente usado.

- Problemas restantes de arquitectura, como la falta de acuerdo para un soporte adecuado de IPv6 multihoming.

Ventajas:

- Convivencia con IPv4, que hará posible una migración suave.
- Gran cantidad de direcciones, que hará virtualmente imposible que queden agotadas. Se estima que si se repartiesen en toda la superficie de la Tierra habría $6.67x10^{23}$ IPs por m^2.
- Direcciones unicast, multicast y anycast.
- Formato de cabecera más flexible que en IPv4 para agilizar el encaminamiento.
- Nueva etiqueta de flujo para identificar paquetes de un mismo flujo.
- No se usa checksum.
- La fragmentación y reensamblado se realiza en los nodos finales, y no en los routers como en IPv4.
- Nuevas características de seguridad. IPSEC formará parte del estándar.
- Nueva versión de ICMP, que incluye a MLD, el equivalente del IGMP de IPv4.
- Auto configuración de los nodos finales, que permite a un equipo aprender automáticamente una dirección IPv6 al conectarse a la red.
- Movilidad incluida en el estándar, que permitirá cambiar de red sin perder la conectividad.

5.5.5. Transición a IPv6

Para que ocurra la coexistencia, el gran número de nodos (nodos IPv4 ó IPv6) se pueden comunicar utilizando infraestructura IPv4, infraestructura IPv6, o una infraestructura que es la combinación de IPv4 e IPv6. La verdadera migración será lograda cuando todos los nodos IPv4 sean convertidos a nodos IPv6 puros. Sin embargo, para un futuro previsible, la migración practica es conseguida cuando tantos nodos IPv4 posibles sean convertidos a nodos IPv6/IPv4.

5.5.5.1. Compatibilidad de Direcciones

Las siguientes direcciones están definidas para ayudar en la coexistencia de los nodos IPv4 e IPv6:

Direcciones compatibles IPv4 (IPv4-compatible):

Las direcciones IPv4-compatible, 0:0:0:0:0:0:w.x.y.z o ::w.x.y.z (donde w.x.y.z es la representación decimal de una dirección pública IPv4), es usada por los nodos IPv6/IPv4 comunicándose con IPv6 sobre una infraestructura IPv4. Cuando la dirección IPv4-compatible es usada como una dirección IPv6 de destino, el trafico IPv6 es automáticamente encapsulado con un encabezado IPv4 y enviado a su destino utilizando la infraestructura IPv4.

Direcciones mapeadas IPv4 (IPv4-mapped):

La dirección IPv4-mapped, 0:0:0:0:0:FFFF:w.x.y.z, es utilizada para representar un nodo IPv4 a un nodo IPv6. Se usa solamente para representación interna. La dirección IPv4-mapped nunca se usa como dirección de origen o destino para paquetes IPv6. La dirección IPv4-mapped es utilizada por algunas implementaciones IPv6 cuando actúa como un traductor entre nodos IPv4 e IPv6 puros.

Direcciones 6 sobre 4 (6over4):

Las direcciones 6over4 están conformadas de un prefijo de dirección unicast de 64 bit válida y el identificador de interfase ::WWXX:YYZZ (donde WWXX:YYZZ es la representación hexadecimal de w.x.y.z, una dirección IPv4 unicast asignada a una interfase). Un ejemplo de una dirección de vinculo local 6over4 basado en la dirección IPv4 131.107.4.92 es FE80::836B:45C. Las direcciones 6over4 son utilizadas para representar un host cuando se usan mecanismos de túnel automático definidos en el RFC2529.

Direcciones 6 a 4 (6to4):

Las direcciones 6to4 están basadas en el prefijo 2002:WWXX:YYZZ::/48 (donde WWXX:YYZZ es la representación hexadecimal de w.x.y.z, una dirección IPv4 pública asignada a una interfase). El prefijo de la dirección 6to4 representa un sitio cuando se utilizan mecanismos de túnel automático definidos en el RFC3056, también conocido como 6to4.

Direcciones ISATAP:

Las direcciones Intra-site Automatic Túnel Addressing Protocol (ISATAP) están compuestas de un prefijo unicast de 64 bits válido y el identificador de interfase ::0:5EFE:w.x.y.z (donde w.x.y.z es una dirección IPv4 unicast asignada a una interfase). Un ejemplo de una dirección ISATAP de vinculo local es FE80::5EFE:131.107.4.92. ISATAP esta definida en el borrador de Internet llamado "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)" (draft-ietf-ngtrans-isatap-x.txt en http://www.ietf.org/internet-drafts/).

Direcciones Teredo:

Las direcciones Teredo utilizan el prefijo 3FFE:831F::/32. Un ejemplo de una dirección Teredo es 3FFE:831F:CE49:7601:8000:EFFF:62C3:FFFE. Más allá de los primeros 32 bits, las direcciones Teredo son utilizadas para codificar la dirección IPv4 de un servidor Teredo, banderas, y la versión codificada de un puerto y dirección externos de un cliente Teredo. Teredo se define en el

borrador de Internet titulado "Teredo: Tunneling IPv6 over UDP through NATs" (draft-huitema-v6ops-teredo-0*x*.txt en http://www.ietf.org/internet-drafts/).

5.5.5.2. Mecanismos de transición

Para coexistir con una infraestructura IPv4 y para proveer una eventual transición hacia una infraestructura IPv6 pura, los siguientes mecanismos son utilizados:

- Capa IP dual (Dual IP Layer).
- Túnel IPv6 sobre IPv4 (IPv6 over IPv4 tunneling).
- Infraestructura DNS (DNS infrastructure).

Capa IP Dual

La capa IP dual es una implementación del grupo de protocolos TCP/IP que incluye a ambas capas Internet IPv4 e Internet IPv6. Este es el mecanismo utilizado por nodos IPv6/IPv4 por lo tanto la comunicación con nodos IPv4 e IPv6 puede ocurrir. Una capa IP dual contiene una sola implementación de protocolos Host-to-Host tales como TCP y UDP. Todos los protocolos de la capa superior en una implementación de capa IP dual pueden comunicarse sobre IPv4, IPv6 o IPv6 tuneleado en IPv4. La figura 20 muestra la arquitectura de una capa IP dual.

Figura 20: Arquitectura de una capa IP dual.

Túnel IPv6 sobre IPv4

Túnel IPv6 sobre IPv4 es el encapsulamiento de paquetes IPv6 con un encabezado IPv4, de esta manera los paquetes IPv6 pueden ser enviados sobre una infraestructura IPv4. Dentro del encabezado IPv4:

- El campo Protocolo de IPv4 es configurado con el 41 para indicar que es un paquete IPv6 encapsulado.
- Los campos Origen y Destino son configurados con las direcciones IPv4 de los extremos del túnel. Los extremos del túnel son configurados, ya sea manualmente como parte de la interfase del túnel o son automáticamente derivados de la interfaz que envía, de la siguiente dirección que concuerda en la ruta, o las direcciones IPv6 origen y destino en el encabezado IPv6.

La figura 21 muestra como se compone el túnel IPv6 sobre IPv4.

Figura 21: Túnel IPv6 sobre IPv4

INFRAESTRUCTURA DNS

Una infraestructura DNS (Domain Name System, Sistema de nombre de dominio) es necesaria para la coexistencia satisfactoria debido al uso de nombres generalizados para referirse a los recursos de la red. Actualizando la infraestructura DNS consiste en llenar los servidores DNS con registros para soportar resoluciones nombre-dirección y dirección-nombre para IPv6. Luego que la dirección es obtenida mediante la consulta al nombre DNS, el nodo origen debe seleccionar cual dirección utilizar para la comunicación.

La infraestructura DNS debe tener los siguientes recursos para la resolución satisfactoria de nombre-dirección y dirección-nombre:

- Registros A para nodos IPv4 puros y nodos IPv6/IPv4.
- Registros AAAA para nodos IPv6 puros y nodos IPv6/IPv4.
- Registros PTR en el dominio IN-ADDR.ARPA para nodos IPv4 puros y nodos IPv6/IPv4.
- Registros PTR en el dominio IP6.ARPA para nodos IPv6 puros y nodos IPv6/IPv4.

5.5.5.3. Configuraciones de túneles

El RFC2893 define las siguientes configuraciones de túneles para encaminar tráfico IPv6 entre nodos IPv6/IPv4 sobre infraestructura IPv4:

- Router-to-Router
- Host-to-Router o Router-to-Host
- Host-to-Host

Router-to-router

En la configuración de túneles router-to-router, dos routers IPv6/IPv4 conectan dos infraestructuras IPv4 o IPv6 sobre una infraestructura IPv4. Los extremos del túnel atraviesan un vínculo lógico en el camino entre el origen y el destino. El túnel IPv6 sobre IPv4 entre dos routers actúa como un simple salto. Las rutas entre cada infraestructura IPv4 o IPv6 apuntan al router IPv6/IPv4 en el extremo.

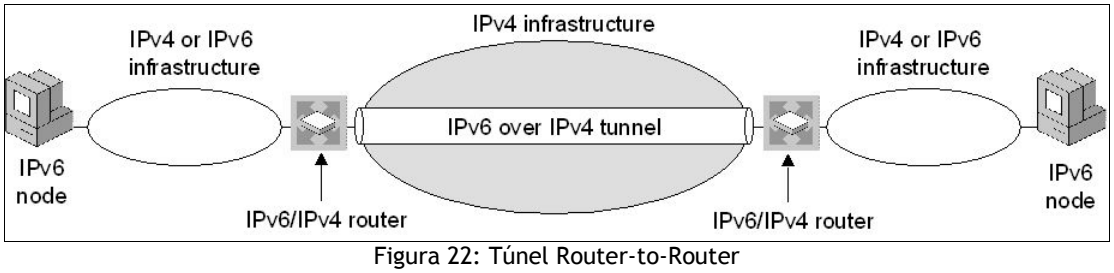


Figura 22: Túnel Router-to-Router

Ejemplos de esta configuración de túnel son:

- Dos dominios IPv6 puros que atraviesan la Internet IPv4.
- Un router 6to4 que atraviesa la Internet IPv4 para alcanzar otro router 6to4 ó un relay router 6to4.

Host-to-router y router-to-host

En la configuración host-to-router, un nodo IPv6/IPv4 que reside dentro de una infraestructura IPv4 crea un túnel IPv6 sobre IPv4 para alcanzar un router IPv6/IPv4. Los extremos atraviesan el primer segmento del camino entre el nodo origen y el nodo destino. El túnel IPv6 sobre IPv4 entre el nodo IPv6/IPv4 y el router IPv6/IPv4 actúa como un solo salto.

En la configuración de túnel router-to-host, un router IPv6/IPv4 crea un túnel IPv6 sobre IPv4 a través de una infraestructura IPv4 para alcanzar un nodo IPv6/IPv4. Los extremos del túnel atraviesan el último segmento del camino entre el nodo de origen y el nodo destino. El túnel IPv6 sobre IPv4 entre el router IPv6/IPv4 y el nodo IPv6/IPv4 actúa como un solo salto.

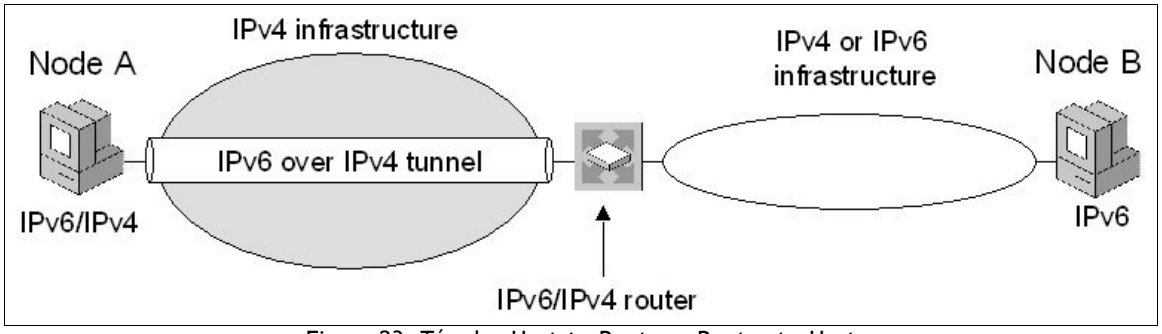


Figura 23: Túneles Host-to-Router y Router-to-Host

Ejemplos de estos túneles son:

- Un host IPv6/IPv4 que cruza una infraestructura IPv4 para alcanzar el Internet IPv6.
- Un host ISATAP que atraviesa una red IPv4 hacia un router ISATAP para alcanzar la Internet IPv4, otra red IPv4 o una red IPv6.

- Un router ISATAP que atraviesa un túnel en una red IPv4 para alcanzar un host ISATAP.

Host-to-host

En la configuración de túneles host-to-host, un nodo IPv6/IPv4 que reside dentro de una infraestructura IPv4 crea un túnel IPv6 sobre IPv4 para alcanzar otro nodo IPv6/IPv4 que reside dentro de la misma infraestructura IPv4. Los extremos del túnel atraviesan el camino entre el nodo de origen y el nodo de destino. El túnel IPv6 sobre IPv4 entre el nodo IPv6/IPv4 actúa como un solo salto.

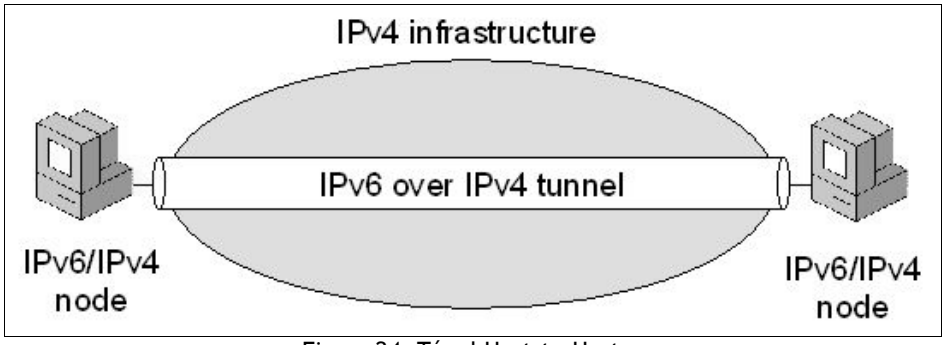


Figura 24: Túnel Host-to-Host

Ejemplos de estos túneles host-to-host son:

- Dos host IPv6/IPv4 que usan direcciones ISATAP para atravesar una infraestructura IPv4.
- Dos host IPv6/IPv4 que utilizan direcciones compatibles IPv4 para atravesar túneles en una infraestructura IPv4.

5.5.5.4. Tipos de túneles

El RFC2893 define los siguientes tipos de túneles:

- Configurados
- Automáticos

Túneles configurados

Un túnel configurado requiere configuración manual de los extremos del túnel. En un túnel configurado, las direcciones IPv4 de los extremos del túnel no son derivados de direcciones que son codificadas en las direcciones de origen o destino IPv6 o en la dirección del siguiente salto en la ruta.

Generalmente, los túneles router-to-router son manualmente configurados. La configuración de la interfase del túnel, consistente de direcciones IPv4 de los extremos del túnel, deben ser manualmente especificados junto con rutas estáticas que usen la interfase del túnel.

Túneles automáticos

Un túnel automático es un túnel que no requiere configuración manual. Los extremos del túnel son determinados por el uso de interfases lógicas de túneles, rutas, y direcciones de origen y destino IPv6.

Las siguientes tecnologías son túneles automáticos:

- 6to4
- ISATAP
- IPv6 Automatic Tunneling
- 6over4
- Teredo

6to4

6to4 es una tecnología de asignación de direcciones y túneles automáticos router-to-router que se utiliza para proveer conectividad IPv6 unicast entre sitios IPv6 y hosts a través del Internet IPv4. 6to4 usa el prefijo de dirección global:

2002:WWXX:YYZZ::/48

Donde WWXX:YYZZ es la representación hexadecimal de una dirección IPv4 pública (w.x.y.z) asignada a un sitio o host. La dirección 6to4 completa es:

2002:WWXX:YYZZ:SubnetID:InterfaceID

Cuando se tienen hosts 6to4, infraestructura de ruteo IPv6, routers 6to4, los siguientes tipos de comunicación son posibles:

- Un host 6to4 se puede comunicar con otro host 6to4 dentro del mismo sitio.
- Un host 6to4 se puede comunicar con otros hosts 6to4 en otros sitios a través del Internet IPv4.
- Un host 6to4 se puede comunicar con otros hosts en la Internet IPv6.

Todos estos tipos de comunicación utilizan tráfico IPv6 sin necesitar obtener ya sea una conexión directa al Internet IPv6 o un prefijo de dirección global IPv6 de un proveedor de este servicio.

ISATAP

ISATAP es una tecnología de asignación de direcciones y túneles automáticos host-to-host, host-to-router, y router-to-host que es utilizada para proveer conectividad IPv6 unicast entre hosts IPv6 a través de una intranet IPv4. Los hosts ISATAP no requieren alguna configuración manual y crean direcciones ISATAP usando mecanismos de auto configuración estándar.

ISATAP puede ser usado para comunicación entre nodos IPv6/IPv4 en una red IPv4. Las direcciones ISATAP utilizan el identificador de interfase localmente administrado ::0:5EFE:w.x.y.z, donde w.x.y.z es cualquier dirección IPv4 unicast, y que incluye ambas direcciones públicas y privadas.

TEREDO

Teredo, también conocido como IPv4 network address translator (NAT) traversal (NAT-T) para IPv6, provee asignación de direcciones y túneles automáticos host-to-host para conectividad IPv6 unicast a través del Internet IPv4 cuando los hosts IPv6/IPv4 están ubicados detrás de uno o múltiples NAT IPv4. Para cruzar los NAT IPv4, los paquetes IPv6 son enviados como mensajes UDP (User Datagram Protocol) IPv4.

6to4 provee una función similar a Teredo; sin embargo, requiere un router con soporte 6to4 en el dispositivo del borde conectado a Internet. La funcionabilidad del router 6to4 no es completamente soportada por NATs IPv4. Aún si el NAT fuese 6to4 activado, podría no funcionar para configuraciones donde existen múltiples NAT entre el sitio e Internet.

Teredo esta diseñado como un último recurso de tecnología de transición para conectividad IPv6. Si la conectividad IPv6 nativo, 6to4 o ISATAP están presentes entre los nodos que se están comunicando, Teredo no es utilizado. Mientras más NAT IPv4 sean actualizados para soportar 6to4 y conectividad IPv6, Teredo será utilizado cada vez menos hasta, eventualmente, dejar de utilizarse.

5.5.6. Migrando a IPv6

La migración de IPv4 a IPv6 es un largo proceso y algunos detalles de la migración son puestos a consideración. A continuación se describe una metodología general para migrar IPv4 hacia IPv6:

1. Actualizar las aplicaciones para ser independientes del protocolo IPv6 o IPv4: Las aplicaciones deben ser cambiadas para poder utilizar la nueva interfase de programación para aplicaciones (API's) para Windows

Socket, de tal manera que se utilicen los resoluciones de nombres, creación de socket, y otras funciones independientes de si es IPv4 o IPv6.

2. Actualizar la infraestructura DNS para soportar direcciones IPv6 y registros PTR: La infraestructura DNS necesita ser actualizada para soportar los nuevos registros AAAA y los registros PTR en el dominio inverso IP6.ARPA (Opcional).
3. Actualizar los hosts a nodos IPv6/IPv4: Los hosts deben ser actualizados para utilizar la capa IP dual o la pila IP dual. Se debe agregar soporte para resolver DNS para poder procesar los resultados a consultas DNS conteniendo direcciones IPv4 e IPv6.
4. Actualizar la infraestructura de ruteo para ruteo IPv6 nativo: Los routers deben ser actualizados para soportar ruteo IPv6 nativo y protocolos de ruteo IPv6.
5. Convertir los nodos IPv6/IPv4 a nodos IPv6 puros: Los nodos IPv6/Ipv4 pueden ser actualizados a nodos IPv6 puros. Este debe ser un objetivo a largo plazo porque puede tomar varios años para todos los dispositivos actualmente IPv4 puros para ser actualizados a IPv6 puros. Para aquellos nodos IPv4 puros que no puedan ser actualizados a IPv6/Ipv4 o IPv6 puros, emplear gateways de traducción para que de esta manera se puedan comunicar con los nodos IPv6 puros.

5.5.7. Asignación de direcciones IPv6

La obtención o asignación de direcciones IPv6 esta regulada de forma similar a las direcciones IPv4, donde existe una organización encargada de su administración. Esta organización es el Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC, Latin American and Caribbean Internet Addresses Registry) que se encarga de administrar el espacio de direcciones IP, Números de Sistemas Autónomos (ASN), Resolución Inversa y otros recursos

para la región de América Latina y el Caribe (LAC) en nombre de la comunidad de Internet.

El proceso de registro de direcciones IPv6 se describe de forma detallada en el sitio Web de la organización (http://lacnic.net/sp/registro/index.html). En la tabla 10 se detallan los precios de asignación de IPv6.

Tabla 11: Precios de asignación de IPv6

TAMAÑO	MONTO INICIAL	MONTO RENOVACIÓN
≤ /32	$ 2,500.00	$ 2,500.00
> /32	$ 20,000.00	$ 20,000.00

En la actualidad y hasta nueva resolución del directorio de LACNIC, las organizaciones que califiquen para recibir bloques de direcciones IPv6 estarán exonerados de pago. Esta medida se toma como una forma de promoción de la adopción de IPv6 en la región de cobertura de LACNIC.

Para el caso de usuarios finales, LACNIC presenta además otra tabla de precios de asignación.

Tabla 12: Precios de asignación de IPv6 para usuarios finales

TAMAÑO	MONTO INICIAL	MONTO ANUAL MANTENIMIENTO
≤ /19	$ 2,500.00	$ 400.00
/18	$ 5,000.00	$ 400.00
/17	$ 7,500.00	$ 400.00
/16	$ 10,000.00 cada /16	$ 400.00

LACNIC otorga un descuento de 50% en los montos de membresía, a Organizaciones no gubernamentales sin fines de lucro, que a juicio de la organización sean consideradas como Usuarios Finales. En este último caso los descuentos en la asignación de direcciones IP aplicaran solamente si dichos recursos son o serán utilizados en servicios que no tengan fines de lucro.

5.5.8. Aplicaciones que utilizan IPv6

Actualmente existen varios proyectos de aplicaciones que soportan IPv6, un ejemplo de esto es el nuevo sistema operativo de Microsoft, Windows Vista, que se ha diseñado para soportar IPv6 de forma nativa.

A continuación se presenta una lista de aplicaciones con soporte a IPv6.

Tabla 13: Aplicaciones con soporte IPv6

NOMBRE	CATEGORIA	DIRECCIÓN
Microsoft Windows XP SP2	Sistema Operativo	http://www.microsoft.com/windowsxp
ASTEC-X 4.00	X Server	http://www.astec-x.com
SSH	Cliente VPN	http://www.ssh.com
Sendmail 8.12	SMTP Server	http://www.sendmail.org
Apache 2.2.3	Web Server	http://httpd.apache.org
Orenosv	Web/Ftp Server	http://hp.vector.co.jp/authors/VA027031/orenosv/index_en.html
TeraTerm Pro 2.3	Cliente Telnet	http://win6.jp/TeraTerm/index.html
FFFTP 1.92a	Cliente FTP	http://www2.biglobe.ne.jp/~sota/ffftp-e.html
Session Directory	Herramienta multicast	http://www-mice.cs.ucl.ac.uk/multimedia/software/sdr
Cygwin IPv6	Librería API para Unix	http://win6.jp/Cygwin/index.html
Fnord!	Web Server	http://sourceforge.net/projects/msfnord
RAT v4	Audio conferencia	http://www-mice.cs.ucl.ac.uk/multimedia/software/rat
VIC	Video conferencia	http://www-mice.cs.ucl.ac.uk/multimedia/software/vic
VLC Media Player	Video streaming	http://www.videolan.org
KVirc	Cliente IRC	http://www.kvirc.net

5.6. FUNCIONAMIENTO DE LA INTEGRACION DE LA RED AVANZADA

Como se observó en los apartados del capítulo 4, existe una infraestructura de red definida y configurada para transmitir la información tanto de la red de Internet como de la Red Avanzada en la Universidad Don Bosco.

Esta infraestructura es capaz además, de soportar una serie de tecnologías como las descritas en los apartados anteriores de este capítulo. El aprovechamiento de la infraestructura y dichas tecnologías depende de la forma como se integren las necesidades de los usuarios con el funcionamiento de la red de la institución.

Para utilizar la red Internet en conjunto con la Red Avanzada, una computadora de usuario final no necesita ser configurada de manera especial. Esto es porque, debido a la forma como se ha diseñado la infraestructura de la red, el router del núcleo se encarga de decidir a donde se debe dirigir la información en base a la dirección destino. Esto se logra por medio de tablas de enrutamiento.

Esto es para el caso específico de la Universidad Don Bosco, donde se están utilizando IPv4 para conectarse tanto a la red Internet como a la Red Avanzada; la computadora del usuario final no necesita tener más que una conexión física a la red institucional.

Cuando se tenga implementada la Red Avanzada sobre IPv6, la computadora del usuario final requerirá tener, además de la IPv4 actual que le da acceso a la red Internet, una IPv6 configurada adicionalmente en su interfase de red para poder acceder a las Redes Avanzadas.

Esto significa también que las computadoras conectadas a la red institucional pueden acceder a otras Redes Avanzadas utilizando los navegadores normales, pero siempre y cuando las instituciones de otras redes avanzadas tengan sitios que puedan ser visualizados por medio de estos programas y, además es necesario conocer la dirección específica para que el router pueda decidir por que enlace saldrá la información.

La única restricción para poder realizar esto es que las redes avanzadas de otras instituciones estén basadas en IPv4 como lo hace la Red Avanzada de la Universidad Don Bosco. Si la dirección que se desea acceder esta sobre IPv6 será necesario utilizar un programa navegador que soporte dicha tecnología y la red deberá ser capaz de utilizar los mecanismos de transición para conectarse a redes IPv6.

Existen ciertas herramientas disponibles para los usuarios finales donde ellos mismos pueden verificar si sus respectivas computadoras están o no utilizando la Red Avanzada de la institución. Estas herramientas son accesadas por medio de navegadores normales, como por ejemplo el Internet Explorer, y se encuentran en la dirección Web: http://e2e.reuna.cl/reuna2/portal.htm.

CONCLUSIONES

- Las redes avanzadas se están consolidando en El Salvador a través de las iniciativas de diversas universidades, entre ellas la Universidad Don Bosco, guiados por las proyecciones de RAICES.
- El futuro económico de las redes avanzadas en El Salvador dependerá de la estimulación en la generación de proyectos propios que permitan el autofinanciamiento de dichas redes.
- La implementación de una red avanzada representa un gasto significativo para cualquier institución. Por ejemplo, el gasto inicial de instalación es de aproximadamente $ 6,500.00; luego hay que agregar el gasto mensual del servicio de conexión y el pago del personal encargado de la red.
- La Universidad Don Bosco posee una infraestructura de red conformada por equipo capaz de soportar las actuales tecnologías de Redes Avanzadas, pero también la red tiene la capacidad de soportar equipo más moderno para, además, mejorar las capacidades de desempeño de dichas tecnologías.
- La integración de la red avanzada en la Universidad Don Bosco es un proceso bastante sencillo debido a que la configuración de la red hace la mayor parte del trabajo; solamente es necesario tener una PC conectada a la red que proporciona el acceso a la Red Avanzada. Para el usuario esta configuración es transparente y no representa un obstáculo en el desempeño de sus actividades diarias.
- La posibilidad de utilizar IPv6 en un futuro dentro de la Red Avanzada de la Universidad Don Bosco representará un cambio en la configuración de las computadoras conectadas a dicha red. Se necesitará tener una IPv4 para acceder al Internet comercial y además será necesario tener una IPv6 para acceder a las redes avanzadas.

- La capacidad de integración de las redes avanzadas permitirá el mejoramiento tecnológico de las actuales redes institucionales aunque la transición hacia las nuevas tecnologías signifique estudios bien planeados y a largo plazo.
- El beneficio de poseer acceso a las Redes Avanzadas es grande ya que proporciona un medio de desarrollo tecnológico para la Universidad Don Bosco, permite que se utilicen nuevas tecnologías en el proceso educativo de los estudiantes y además proporciona un medio de experimentación que además de mejorar la capacidad técnica de la universidad también puede mejorar su capacidad económica por medio de productos propios resultado de dicha experimentación.
- Para que las tecnologías descritas en esta investigación puedan ser utilizadas correctamente dentro de la red de la Universidad Don Bosco, es necesario hacer estudios adecuados ya que no solo se estará afectando la red avanzada, sino también la red Internet que es donde los usuarios se desenvuelven mayormente.
- La red avanzada de la Universidad Don Bosco utilizando IPv4 necesita tecnología de túneles para comunicarse con redes avanzadas que utilicen IPv6, para el caso una opción sería la de utilizar un túnel 6to4 o uno ISATAP en una configuración Host-to-router y router-to-host. El túnel 6to4 para el caso de utilizar direcciones IPv4 públicas o el ISATAP para el caso de utilizar direcciones IPv4 públicas y privadas.

GLOSARIO

- **ATM:** (Asynchronous Transfer Mode, Modo de Transferencia Asíncrona) es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones. Con esta tecnología, a fin de aprovechar al máximo la capacidad de los sistemas de transmisión, sean estos de cable o radioeléctricos, la información no es transmitida y conmutada a través de canales asignados en permanencia, sino en forma de cortos paquetes (celdas ATM) de longitud constante y que pueden ser enrutadas individualmente mediante el uso de los denominados canales virtuales y trayectos virtuales.
- **Backbone**: Mecanismo de conectividad primario en un sistema distribuido. Todos los sistemas que tengan conexión al backbone (columna vertebral) pueden interconectarse entre sí, aunque también puedan hacerlo directamente o mediante redes alternativas.
- **Dark Fiber:** En telecomunicaciones, la fibra oscura o dark fiber (o la Fibra) es el nombre dado a los cables de fibra ópticos que todavía no se utilizarán pero se han puesto. Ellos por lo tanto todavía no están conectados con cualquier dispositivo, y están solamente allí para uso futuro.
- **Dirección MAC:** En redes de computadoras la dirección MAC (Media Access Control address) es un identificador hexadecimal de 48 bits que se corresponde de forma única con una tarjeta o interfaz de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (los primeros 24 bits) y el fabricante (los 24 bits restantes). MAC opera en la capa 2 del modelo OSI, encargada de hacer fluir la información libre de errores entre dos máquinas conectadas directamente. Para ello se generan tramas, pequeños bloques de

información que contienen en su cabecera las direcciones MAC correspondiente al emisor y receptor de la información.

- **DWDM:** (Dense Wavelength Division Multiplexing, Multiplexación por división en longitudes de onda densas) es un método de multiplexación muy similar a la Multiplexación por división de frecuencia que se utiliza en medios de transmisión electromagnéticos. Varias señales portadoras (ópticas) se transmiten por una única fibra óptica utilizando distintas longitudes de onda de un haz láser cada una de ellas. De esta manera se puede multiplicar el ancho de banda efectivo de la fibra óptica, así como facilitar comunicaciones bidireccionales. Para transmitir mediante DWDM es necesario dos dispositivos complementarios: un multiplexador en lado transmisor y un demultiplexador en el lado receptor.
- **Ethernet**: Norma o estándar (IEEE 802.3) que determina la forma en que los puestos de la red envían y reciben datos sobre un medio físico compartido que se comporta como un bus lógico, independientemente de su configuración física. Originalmente fue diseñada para enviar datos a 10 Mbps, aunque posteriormente ha sido perfeccionado para trabajar a 100 Mbps, 1 Gbps o 10 Gbps y se habla de versiones futuras de 40 Gbps y 100 Gbps.
- **Jitter:** variación en la cantidad de latencia entre paquetes de datos recibidos.
- **Multicast**: (multidifusión). En el sistema multicast la transmisión de información llega a múltiples puntos a la vez. Modo de difusión de información en vivo que permite que ésta pueda ser recibida por múltiples nodos de la red y por lo tanto por múltiples usuarios.
- **RFC:** (Request For Comments) Conjunto de notas técnicas y organizativas donde se describen los estándares o recomendaciones de Internet (originalmente ARPANET), comenzado en 1969.En el caso de la informática, están hechos para hacer compatibles los programas entre sí y que se pueda usar diferente software para la misma función. Definen

protocolos y lenguajes, que garantizan la interoperabilidad entre sistemas si ambos cumplen el mismo RFC.

- **Router**: (enrutador o encaminador) es un dispositivo hardware o software de interconexión de redes de computadoras que opera en la capa 3 (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando como base la información de la capa de red. En general, debe considerarse como el elemento responsable de discernir cuál es el camino más adecuado para la transmisión de mensajes en una red compleja que está soportando un tráfico intenso de datos.
- **RPF:** (Reverse Path Forwarding) es una técnica utilizada en ruteo multicast. Es utilizada para construir rutas de envío de origen específico (SPT, Shortest Path Tree), en las cuales el tráfico puede fluir más eficientemente.
- **Switch**: (conmutador) es un dispositivo de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconnection). Este interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de una red a otra, de acuerdo con la dirección MAC de destino de los datagramas en la red.
- **Tele inmersión**: Emplea sistemas avanzados de telecomunicación de alta velocidad, lo cual permite captar los movimientos y otros aspectos de los usuarios y que se retransmitan a través de una red de alta velocidad. Las personas pueden manipular datos, compartir simulaciones y experiencias como si estuvieran reunidas físicamente. Requiere gran ancho de banda, poco retardo y una mínima pérdida de datos en la red.
- **UNI:** (User to Network Interface o interfaz usuario a red), formato de celda ATM más utilizado.

FUENTES DE INFORMACIÓN

Bibliografía:

- **Handbook of Virtual Environments: Design, Implementation, and Applications**
  Stanney, Kay M.
  Lawrence Erlbaum Associates
  2002.
- **Cisco CCNA Exam #640 – 507 Certification Guide**
  Odom, Wendell
  Lacidar Unlimited, Inc.
  2000.
- **Cisco Certified Network Associate Study Guide**
  Lammle, Todd
  SYBEX, Inc., Segunda edición
  2000.
- **Manual de Redes**
  Moreno, Luciano
  BJS Software, España
  2000.
- **Internet en El Salvador**
  Ibarra Fernández, Rafael Antonio
  2002.
- **Boletín DeClara**
  Año 1 - No 5
  2005.
- **Trabajo sobre convertidores**
  Gil Rodríguez, Francisco José
  Universidad de Las Palmas de Gran Canaria
  2003.

- **Arquitectura de IP Multicast para backbone de Internet2**
  Castañeda, Ricardo; López, Max; Servín, Arturo
  2003
- **Guía de Implementación de Multicast para Internet2**
  Servín, Arturo
  2003
- **Quality of Service Technical White Paper**
  Microsoft Corporation
  1999
- **Calidad de Servicio (QoS)**
  Montañana, Rogelio
  Universidad de Valencia
  2004
- **Modelo de evaluación de QoS para una red de Campus**
  Martínez, Juan Antonio
  RedIris (España)
  2003
- **IPv6 Transition Technologies**
  Microsoft Corporation
  2005

Direcciones Electrónicas:

- **Hobbes' Internet Timeline**
  http://www.zakon.org/robert/internet/timeline
- **Cooperación Latinoamericana de Redes Avanzadas**
  http://www.redclara.org
- **Red Académica de Centros de Investigación y Universidades Nacionales de Alta Velocidad**
  http://www.reacciun2.edu.ve

- **Corporación Universitaria para el Desarrollo de Internet**
  http://www.cudi.edu.mx
- **Red Avanzada de Investigación, Ciencia y Educación Salvadoreña**
  http://www.raices.org.sv
- **Internet2**
  http://www.profc.udec.cl/internet2
- **RFC Editor**
  http://www.rfc-editor.org/
- **Internet Protocol Multicast**
  http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ipmulti.htm
- **Tecnologías Colaborativas Populares**
  http://www.videnet.gatech.edu/cookbook.es/list_page.php?topic=3&url=H323_hardware.htm&level=1&sequence=1&name=H.323
- **IPv6 Guide for Windows Sockets Applications**
  http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winsock/winsock/ipv6_guide_for_windows_sockets_applications_2.asp
- **Network Protocols Development**
  http://msdn.microsoft.com/library/default.asp?url=/library/en-us/qos/qos/qos_functions.asp

ANEXOS

ANEXO 1: TECNOLOGÍA DE LA RED DE LA UNIVERSIDAD DON BOSCO

Ethernet es la tecnología de red LAN más usada, resultando idónea para aquellos casos en los que se necesita una red local que deba transportar tráfico esporádico y ocasionalmente pesado a velocidades muy elevadas. Las redes Ethernet se implementan con una topología física de estrella y lógica de bus, y se caracterizan por su alto rendimiento a grandes velocidades.

El origen de las redes Ethernet hay que buscarlo en la Universidad de Hawai, donde se desarrollo, en los años setenta, el **Método de Acceso Múltiple con Detección de Portadora y Detección de Colisiones, CSMA/CD** (Carrier Sense and Multiple Access with Collition Detection), utilizado actualmente por Ethernet. Este método surgió ante la necesidad de implementar en las islas Hawai un sistema de comunicaciones basado en la transmisión de datos por radio, que se llamó Aloha, y permite que todos los dispositivos puedan acceder al mismo medio, aunque sólo puede existir un único emisor encada instante. Con ello todos los sistemas pueden actuar como receptores de forma simultánea, pero la información debe ser transmitida por turnos.

El centro de investigaciones PARC (Palo Alto Research Center) de la Xerox Corporation desarrolló el primer sistema Ethernet experimental en los años 70, que posteriormente sirvió como base de la especificación 802.3 publicada en 1980 por el Institute of Electrical and Electronic Engineers (IEEE).

Las redes Ethernet son de carácter no determinista, en la que los hosts pueden transmitir datos en cualquier momento. Antes de enviarlos, escuchan el medio de transmisión para determinar si se encuentra en uso. Si lo está, entonces esperan. En caso contrario, los host comienzan a transmitir. En caso de que dos o más host empiecen a transmitir tramas a la vez se producirán encontronazos o choques entre tramas diferentes que quieren pasar por el mismo sitio a la vez. Este fenómeno se denomina **colisión**, y la porción de los

medios de red donde se producen colisiones se denomina **dominio de colisiones.**

Tipos de redes Ethernet

Existen por lo menos 18 variedades de Ethernet, relacionadas con el tipo de cableado empleado y con la velocidad de transmisión.

Variedades de red Ethernet

Tipo	Medio	Ancho de banda máximo	Longitud máxima de segmento	Topología Física	Topología Lógica
10Base5	Coaxial grueso	10 Mbps	500 m	Bus	Bus
10Base-T	UTP Cat 5	10 Mbps	100 m	Estrella; Estrella Extendida	Bus
10Base-FL	Fibra óptica multimodo	10 Mbps	2.000 m	Estrella	Bus
100Base-TX	UTP Cat 5	100 Mbps	100 m	Estrella	Bus
100Base-FX	Fibra óptica multimodo	100 Mbps	2.000 m	Estrella	Bus
1000Base-T	UTP Cat 5	1000 Mbps	100 m	Estrella	Bus

En el caso de la Universidad Don Bosco se esta utilizando el tipo 100 Base-FX conocido como Fast Ethernet.

Las redes 100 Base-Fx (IEEE 802.3u) se crearon con la idea de paliar algunos de los fallos contemplados en las redes Ethernet 10 Base-T y buscar una alternativa a las redes FDDI (Fiber Distributed Data Interface - Interfaz de Datos Distribuida por Fibra), y están basadas en una *topología en estrella para fibra óptica*. Con objeto de hacerla compatible con Ethernet 10 Base-T, la tecnología Fast Ethernet preserva los formatos de los paquetes y las interfaces, pero aumenta la rapidez de transmisión hasta los 100 Mbps. En la redes Fast

Ethernet se usan cables de cuatro pares trenzados de la clase 3, uno de los cuales va siempre al hub central, otro viene siempre desde el hub, mientras que los otros dos pares son conmutables. En cuanto a la codificación de las señales, se sustituye la codificación Manchester por señalización ternaria, mediante la cual se pueden transmitir 4 bits a la vez. También se puede implementar Fast Ethernet con cableado de la clase 5 en topología de estrella (100 Base-TX), pudiendo entonces soportar hasta 100 Mbps con transmisión full dúplex.

ANEXO 2: FIBRA ÓPTICA EN LA RED DE LA UNIVERSIDAD DON BOSCO

Las redes FDDI (Fiber Distributed Data Interface - Interfaz de Datos Distribuida por Fibra) surgieron a mediados de los años ochenta para dar soporte a las estaciones de trabajo de alta velocidad, que habían llevado las capacidades de las tecnologías Ethernet y Token Ring existentes hasta el límite de sus posibilidades.

Están implementados mediante una topología física de estrella (lo más normal) y lógica de anillo doble de token, uno transmitiendo en el sentido de las agujas del reloj (anillo principal) y el otro en dirección contraria (anillo de respaldo o back up), que ofrece una velocidad de 100 Mbps sobre distancias de hasta 200 metros, soportando hasta 1000 estaciones conectadas. Su uso más normal es como una tecnología de backbone para conectar entre sí redes LAN de cobre o computadores de alta velocidad.

Las redes FDDI utilizan un mecanismo de transmisión de tokens similar al de las redes Token Ring, pero además, acepta la asignación en tiempo real del ancho de banda de la red, mediante la definición de dos tipos de tráfico:

1. **Tráfico Síncrono**: Puede consumir una porción del ancho de banda total de 100 Mbps de una red FDDI, mientras que el tráfico asíncrono puede consumir el resto.
2. **Tráfico Asíncrono**: Se asigna utilizando un esquema de prioridad de ocho niveles. A cada estación se asigna un nivel de prioridad asíncrono.

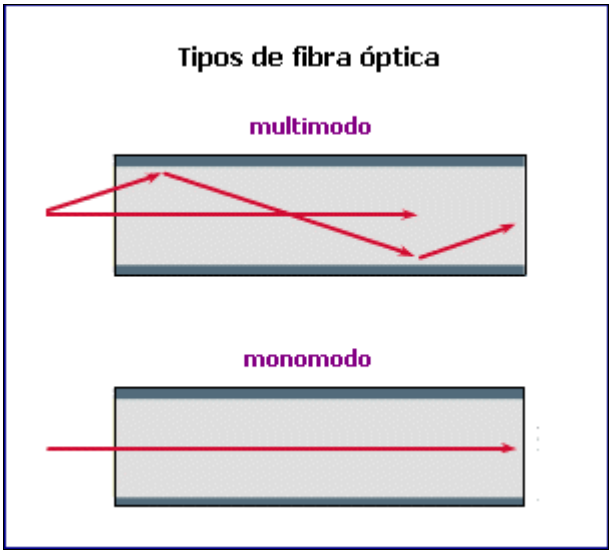
El ancho de banda síncrono se asigna a las estaciones que requieren una capacidad de transmisión continua. Esto resulta útil para transmitir información de voz y vídeo. El ancho de banda restante se utiliza para las transmisiones asíncronas.

Las fuentes de señales de los transceptores de la FDDI son LEDs (diodos electroluminiscentes) o láser. Los primeros se suelen usar para tendidos entre máquinas, mientras que los segundos se usan para tendidos primarios de backbone.

Medios en las redes FDDI

Una de las características de FDDI es el uso de la fibra óptica como medio de transmisión. La fibra óptica ofrece varias ventajas con respecto al cableado de cobre tradicional, por ejemplo:

- Seguridad: la fibra no emite señales eléctricas que se pueden interceptar.
- Confiabilidad: la fibra es inmune a la interferencia eléctrica.
- Velocidad: la fibra óptica tiene un potencial de rendimiento mucho mayor que el del cable de cobre.



Existen dos clases de fibra: monomodo (también denominado modo único); y multimodo. La fibra monomodo permite que sólo un modo de luz se propague a través de ella, mientras que la fibra multimodo permite la

propagación de múltiples modos de luz. Los **modos** se pueden representar como haces de rayos luminosos que entran a la fibra en un ángulo determinado.

Cuando se propagan múltiples modos de luz a través de la fibra, éstos pueden recorrer diferentes distancias, según su ángulo de entrada. Como resultado, no llegan a su destino simultáneamente; a este fenómeno se le denomina **dispersión modal**.

La fibra monomodo puede acomodar un mayor ancho de banda y permite el tendido de cables de mayor longitud que la fibra multimodo. Debido a estas características, la fibra monomodo se usa a menudo para la conectividad entre edificios mientras que la fibra multimodo se usa con mayor frecuencia para la conectividad dentro de un edificio. La fibra multimodo usa los LED como dispositivos generadores de luz, mientras que la fibra monomodo generalmente usa láser. En la Universidad Don Bosco se utiliza la fibra multimodo.

ANEXO 3: CONVERTIDORES DE MEDIO PARA FIBRA ÓPTICA EN LA UNIVERSIDAD DON BOSCO.

Colocando un convertidor de medios, se consigue que un cable se parezca a otro cable, sin cambiar la naturaleza de la red.

Un convertidor de medio es un pequeño aparato con dos interfaces de medios dependientes y una fuente de alimentación. Pueden ser instalados casi en cualquier lugar del entorno de red, expandiéndola en lugar de limitar sus opciones. La infraestructura de la red y la inversión realizada están protegidas. Adaptar nuevos tipos de medio, tales como fibra óptica, no requiere grandes costos de actualización de hardware.

Ventajas de la conversión de medios

El estándar del cableado estructurado se desarrolló para proveer de opciones de cableado para todos los tipos de red. Sin embargo, en la práctica, el estándar tiene limitaciones que hacen que las ampliaciones o migraciones de red resulten difíciles y costosas.

La tecnología de conversión de medios ofrece las siguientes ventajas:

- Posibilidad de añadir nuevos aparatos sin colocar costosos cableados o reemplazar componentes (la inversión en la red está protegida).
- Capacidad para integrar fácilmente la fibra óptica y extender, con ello, las distancias de la red hasta donde se necesite.
- Capacidad de proveer de un enlace (link) entre distintos tipos de medio que es transparente al usuario final y al administrador de la red.
- Permite seguir cambiando la tecnología, integrar en la red nuevos aparatos de gran ancho de banda, y sin salirse del presupuesto.

Los convertidores de medio convierten un tipo de medio a otro: coaxial a par trenzado, coaxial a fibra óptica, par trenzado a fibra óptica y fibra óptica

monomodo a multimodo. El aparato lleva dos interfaces de medios dependientes y una fuente de alimentación. El tipo de conectores depende de la selección de medio a ser convertido por la unidad. Como los conectores son especificados por el IEEE y son usados para cable estándar, se dice que son **interfaces dependientes de medio**.

Tipos de conversión de medios en Ethernet y Fast Ethernet

Las diferentes conversiones que pueden realizarse entre diferentes tipos de medio se presentan a continuación:

- **10BASE-2 a 10BASE-T:** para conectar un segmento o terminal coaxial Ethernet a un segmento de tipo par trenzado.
- **10BASE2 a 10BASE-FL (Multimodo):** para conectar un segmento coaxial Ethernet a un puerto 10BASE-FL con un conector ST para fibra óptica.
- **10BASE-T a 10BASE-FL (Monomodo):** para conectar un segmento existente 10BASE-T o aparato a un backbone de fibra óptica monomodo Ethernet.
- **10BASE-T a 10BASE-FL (Multimodo):** para conectar un segmento existente 10BASE-T o aparato a un backbone de fibra óptica multimodo Ethernet.
- **100BASE-TX a 100BASE-FX (Multimodo):** para conectar un aparato de par trenzado 100BASE-TX a un puerto de fibra óptica multimodo 100BASE-FX que tiene un conector de fibra óptica ST o SC.
- **100BASE-TX a 100BASE-FX (Monomodo):** para conectar un aparato de par trenzado 100BASE-TX a un puerto de fibra óptica monomodo 100BASE-FX que tiene un conector de fibra óptica ST o SC.
- **100BASE-TX a 100BASE-FX (Bridge):** para conectar en topologías que operan a diferentes velocidades. Se pueden usar dos convertidores de medio del tipo 100BASE-TX a 100BASE-FX bridging para extender la conexión de una red 2000 metros.

Aplicaciones de la conversión de medios

Entre las diferentes aplicaciones que se le pueden dar a la conversión de medios se pueden resaltar las siguientes:

Extender distancias en la red: los convertidores de medio de coaxial a fibra o de par trenzado a fibra permiten conectar un grupo de trabajo (*Workgroups*) a un servidor distante o a un switch central, o extender las distancias entre aparatos (similares o no) tanto en modo full dúplex como en modo half dúplex. Una configuración back-to-back usando cable de fibra permite un método simple para extender la distancia entre un switch (half o full duplex) y un servidor hasta los 2000 metros mediante fibra multimodo y 20.000 metros utilizando fibra monomodo.

Conectar equipos con diferentes tipos de medios en una red existente: por ejemplo, los convertidores de medio 10BASE-T a 10BASE-FL pueden conectar un segmento o equipo existente 10BASE-T, como puede ser una impresora que no soporta una conexión de fibra óptica, a un backbone de fibra óptica Ethernet.

Incorporar tecnología Fast Ethernet en redes Ethernet: Dos Convertidores de Medio 100BASE-TX a 100BASE-FX Bridging pueden ser usados para extender una conexión de red a 2000 metros. Cuando se usa con hubs Fast Ethernet, la conexión de fibra permitirá un enlace a 100Mbps sin colisión y full-duplex entre dos equipos.

Convertidores de medios utilizados en redes Fast Ethernet

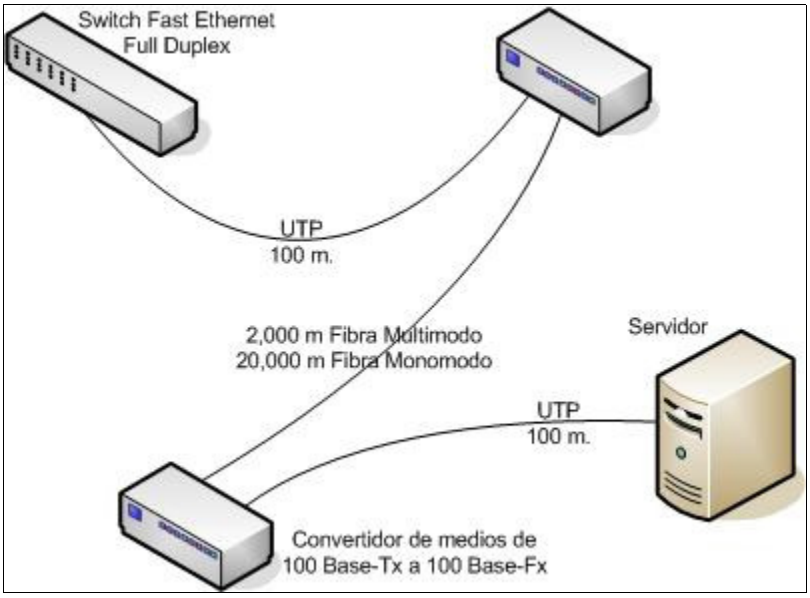
En redes Fast Ethernet, como la de la Universidad Don Bosco, se utilizan los siguientes convertidores de medios:

El convertidor de medios 100 Base-Tx a 100 Base-Fx

Con el convertidor de Medios 100 Base-Tx a 100 Base-Fx, es mucho más sencilla y mejora la relación costo-efectividad de la integración de UTP y fibras ópticas en redes Fast Ethernet. Este convertidor de medios opera mejor en redes dúplex.

Utilizado en pares, este convertidor de medios puede extender distancias entre dos conmutadores de par trenzado o un conmutador y un servidor que estén hasta 2,000 metros en multimodo o hasta 20,000 metros en fibra óptica monomodo.

Un convertidor de medios simple 100BASE-TX a 100BASE-FX puede ser utilizado también para conectar dispositivos remotos. Utilizando un convertidor de medios, un conmutador con puerto de cobre puede ser conectado a otro conmutador con una interfase ya existente de fibra.



Algunas de las especificaciones propias de este convertidor se presentan en la siguiente tabla:

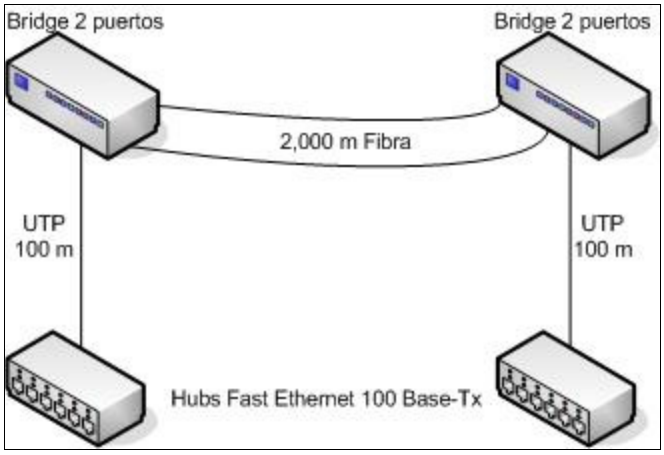
Conectores	1 RJ-45, 1 ST (ó SC) multimodo dúplex ó 1 RJ-45, 1 SC monomodo dúplex
Especificaciones del Conector Monomodo	Longitud de Onda: 1300nm. Potencia de Tx. de la Fibra Óptica: -15.0 dB. Sensibilidad de Recepción de la Fibra Óptica: -32.0 dB. Cable Recomendado: 9/125 μm Fibra Monomodo.
Especificaciones del Conector Multimodo	Longitud de Onda: 1300nm. Potencia de Tx. de la Fibra Óptica: -19.0 dB. Sensibilidad de Recepción de la Fibra Óptica: -32.0 dB. Cable Recomendado: 62.5/125 μm Fibra Multimodo. Opcional: • 100/140 μm Fibra Multimodo • 85/125 μm Fibra Multimodo • 50/125 μm Fibra Multimodo
Distancias Máximas	Fibra Multimodo: 2,000 metros. 100Base-Tx: 100 metros.

El convertidor de medios Bridging 100 Base-Tx a 100 Base-Fx

El convertidor de medios Bridging 100 Base-Tx a 100 Base-Fx, brinda soluciones para **ambientes de conversión semi-dúplex**. Posee dos puertos Ethernet de par trenzado no blindado 10/100 y un puerto de fibra 100 Base-Fx. Ambos puertos RJ-45 son auto sensibles a los 10 Base-T o a los 100 Base-Fx. El puerto de fibra es del tipo ST.

Utiliza tecnología de packet buffering para asegurarse que los paquetes de error sean filtrados. Este convertidor provee 1 Mbyte de packet buffer, cantidad suficiente para sostener un mínimo de 600 paquetes Ethernet que hayan sido maximizados, asegurando un ambiente de red más fuerte en cualquier aplicación que requiera de tecnología de conversión de medios, lo cual es llevado a cabo a las velocidades del cable en cualquier configuración.

Dos convertidores de medios Bridging Base-Tx a 100 Base-Fx pueden ser utilizados para extender una conexión de redes hasta 2,000 metros. Cuando es utilizado como hubs Fast Ethernet, la fibra proveerá una conexión sin colisiones entre los dos dispositivos.



Algunas de las especificaciones propias de este convertidor se presentan en la siguiente tabla:

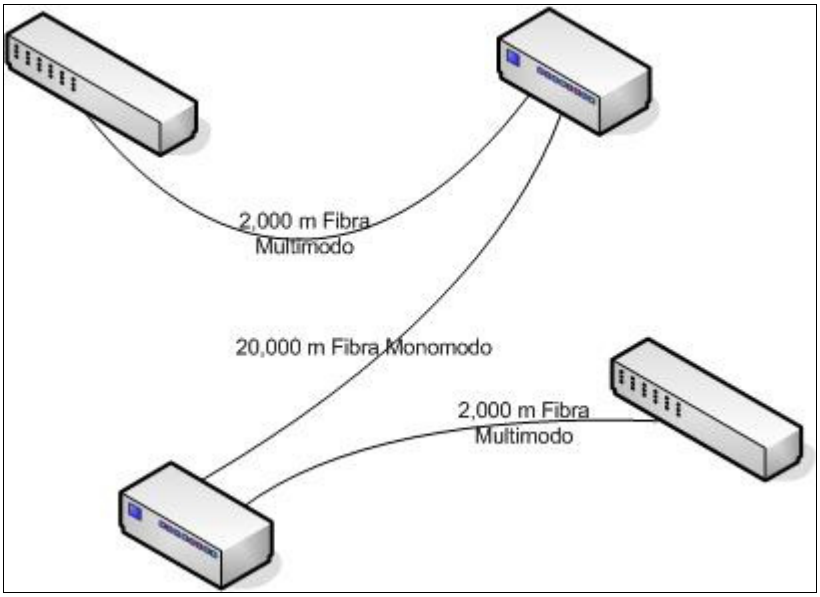
Performance	Velocidad de los paquetes: 10Mbps 14,880pps, 10Mbps 148,800pps.
Modelos	IEEE 802.3
Conectores	2 puertos Ethernet RJ45 10/100. 1 conector fibra multimodo ST 100BASE-FX.
Distancias Máximas	10BASE-T: 100 metros 100BASE-TX: 100 metros 100BASE-FX: 2,000 metros

Switches	Ambos puertos: Habilita la operación a 10 ó 100 Mbps o Dúplex o Semi-dúplex. Selección de Fibra/Cobre en uno de los puertos

El convertidor de medios 1300 nm Monomodo a Multimodo

El convertidor de medios 1300nm Monomodo a Multimodo es ideal para conectar **FDDI**, **Fast Ethernet** o **ATM**, ya que estos protocolos utilizan una longitud de onda de 1300nm por transmisión de fibra óptica. De hecho, cualquier protocolo de red entre 10 Mbps y 155 Mbps puede ser utilizado.

Capaz de extender distancias de hasta 20 km., este convertidor puede ser utilizado en muchos ámbitos.



Algunas de las especificaciones propias de este convertidor se presentan en la siguiente tabla:

Modelos	IEEE 802.3

Conectores	1 dúplex multimodo SC, 1300nm 1 dúplex monomodo SC, 1300nm
Distancias Máximas	Multimodo: 2,000 m. Monomodo: 20,000 m.

ANEXO 4: PROGRAMANDO PARA IPV6 EN WINDOWS

Actualmente, Windows XP y Windows 2003 Server poseen soporte para IPv6, posteriormente, Windows Vista, el nuevo sistema operativo de Microsoft, será creado con soporte para IPv6 de forma nativa.

Configurando el ambiente de desarrollo y las herramientas de programación

Para este caso es necesario utilizar el API Win32 (WinSock2) y el lenguaje C/C++ en Windows XP SP2.

El software necesario para programar es el siguiente:

1. Microsoft Windows XP SP2.
2. Microsoft Visual Studio .NET 2003.
3. Microsoft Platform SDK para Windows 2003 Server SP1.

Sobre el primer punto es necesario preparar el sistema operativo instalando el SP2 para Windows XP, luego hay que instalar el protocolo IPv6 de Windows.

Esto se hace por medio de la línea de comandos. Digitando el comando "cmd" en la casilla de Inicio -> Ejecutar, o seleccionando Inicio -> Programas -> Accesorios -> Símbolo de Sistema.

Luego en la línea de comandos se escribe "ipv6 install" y se presiona Enter. Este comando instala el protocolo en la computadora. Adicionalmente se puede utilizar el comando "netsh interface ipv6 install".

Para verificar que el protocolo fue instalado satisfactoriamente se ejecuta el comando “ping ::1. Si el comando devuelve una respuesta entonces el protocolo fue instalado correctamente.

Acerca del segundo punto, además del Visual Studio .NET 2003 se puede utilizar el Microsoft Visual Studio 6 o superior.

Referente al punto tres, hay que obtener el SDK para Windows 2003 Server desde el sitio de Microsoft. A pesar que el nombre hace referencia a Windows 2003 Server, este trae componentes para Windows XP que son necesarios para desarrollar aplicaciones para WinSock2. El SDK se puede obtener en la siguiente dirección:

http://www.microsoft.com/downloads/details.aspx?FamilyId=A55B6B43-E24F-4EA3-A93E-40C0EC4F68E5&displaylang=en

Durante el proceso de instalación, es necesario asegurarse de seleccionar la opción “Microsoft Windows Core SDK”. Esto incluye los archivos de cabecera (.h) para Win32 API/WinSock, librerías de importación, recursos del compilador y otros.

Luego de instalado, hay que verificar la ruta de búsqueda de la línea de comando (PATH environment variable) y la ruta de búsqueda para los archivos de cabecera (INCLUDE environment variable) y la importación de librerías (LIB environment variable). Los instaladores del Visual Studio y del Platform SDK los configuraran automáticamente, pero es importante el orden. La clave esta en configurarlos de tal manera que las rutas del Platform SDK sean encontradas antes que las del Visual Studio.

A continuación se muestra un ejemplo de cómo debería quedar la configuración de las variables de ambiente:

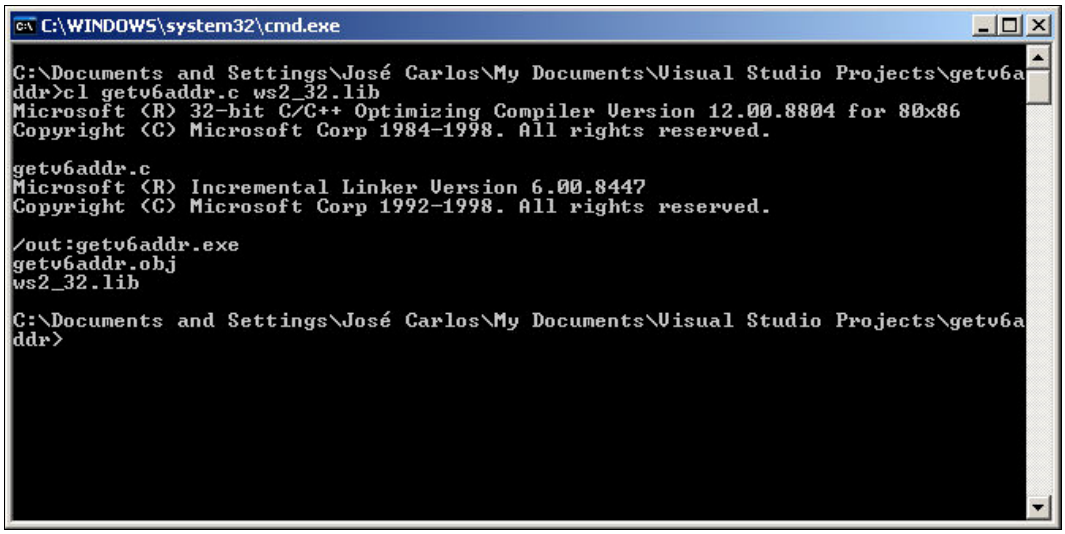
```
•PATH=
  C:\Program Files\Microsoft Platform SDK\Bin;
  ----------------------------------------------
  C:\Program Files\Microsoft Platform SDK\Bin\WinNT;
  ----------------------------------------------------
  C:\Program Files\Microsoft Visual Studio .NET 2003\Common7\IDE;
  C:\Program Files\Microsoft Visual Studio .NET 2003\VC7\BIN;
  C:\Program Files\Microsoft Visual Studio .NET 2003\Common7\Tools;
  C:\Program Files\Microsoft Visual Studio .NET 2003\Common7\Tools\bin\prerelease;
  C:\Program Files\Microsoft Visual Studio .NET 2003\Common7\Tools\bin;
  C:\Program Files\Microsoft Visual Studio .NET 2003\SDK\v1.1\bin;
  C:\Program Files\Microsoft Visual Studio .NET 2003\SDK\v1.1\v1.1.4322

•INCLUDE=
  C:\Program Files\Microsoft Platform SDK\include;
  ------------------------------------------------
  C:\Program Files\Microsoft Visual Studio .NET 2003\VC7\ATLMFC\INCLUDE;
  C:\Program Files\Microsoft Visual Studio .NET 2003\VC7\INCLUDE;
  C:\Program Files\Microsoft Visual Studio .NET 2003\VC7\PlatformSDK\include\prerelease;
  C:\Program Files\Microsoft Visual Studio .NET 2003\VC7\PlatformSDK\include;
  C:\Program Files\Microsoft Visual Studio .NET 2003\SDK\v1.1\include

•LIB=
  C:\Program Files\Microsoft Platform SDK\lib;
  -------------------------------------------
  C:\Program Files\Microsoft Visual Studio .NET 2003\VC7\ATLMFC\LIB;
  C:\Program Files\Microsoft Visual Studio .NET 2003\VC7\LIB;
  C:\Program Files\Microsoft Visual Studio .NET 2003\VC7\PlatformSDK\lib\prerelease;
  C:\Program Files\Microsoft Visual Studio .NET 2003\VC7\PlatformSDK\lib;
  C:\Program Files\Microsoft Visual Studio .NET 2003\SDK\v1.1\lib
```

Utilizando el compilador

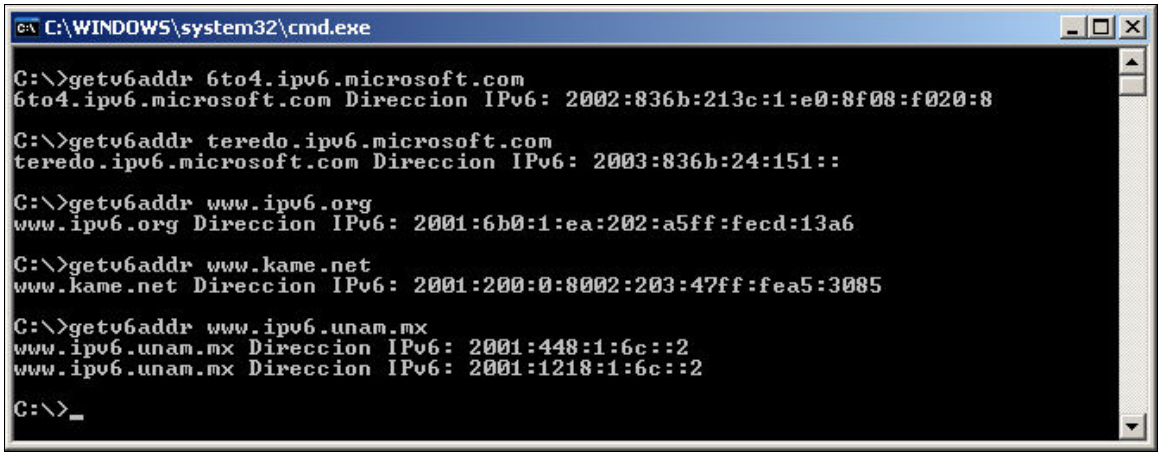
A continuación se muestra la aplicación getv6addr. Getv6addr.exe es un programa que encuentra la dirección IPv6 para un host pasado como argumento. El código del programa (getv6addr.c) es el siguiente:

```c
#include <winsock2.h>
#include <ws2tcpip.h>
#include <stdio.h>

int main(int argc, char *argv[])
{
    char *nodename;
    WSADATA wsaData;
    ADDRINFO hints;
    LPADDRINFO ai, ai0;
    int e;
    /* analizando el argumento en la linea de comando */
    if (argc != 2) {
    fprintf(stderr, "Sintaxis: getv6addr HOSTNAME\n");
    exit(1);
    }
    nodename = argv[1];
    /* inicializando Windows Socket */
    WSAStartup(MAKEWORD(2, 2), &wsaData);
    /* resolviendo "www.host.com" */
    memset(&hints, 0, sizeof(hints));
    hints.ai_family = AF_INET6;
    if (e = getaddrinfo(nodename, NULL, &hints, &ai0)) {
    fprintf(stderr, "%s: %s\n", nodename, gai_strerror(e));
    WSACleanup();
    exit(1);
    }
    /* imprime la dirección IPv6 si la resolucion es satisfactoria */
    for (ai = ai0; ai; ai = ai->ai_next) {
    char v6addrstr[NI_MAXHOST];
    getnameinfo(ai->ai_addr, ai->ai_addrlen,
            v6addrstr, sizeof(v6addrstr),  NULL, 0, NI_NUMERICHOST);

    printf("%s Direccion IPv6: %s\n", nodename, v6addrstr);
    }

    /* limpiar */
    freeaddrinfo(ai0);
    WSACleanup();
}
```

En la siguiente imagen se muestra la secuencia de comandos para compilar el programa:



A continuación se muestra la ejecución del programa:

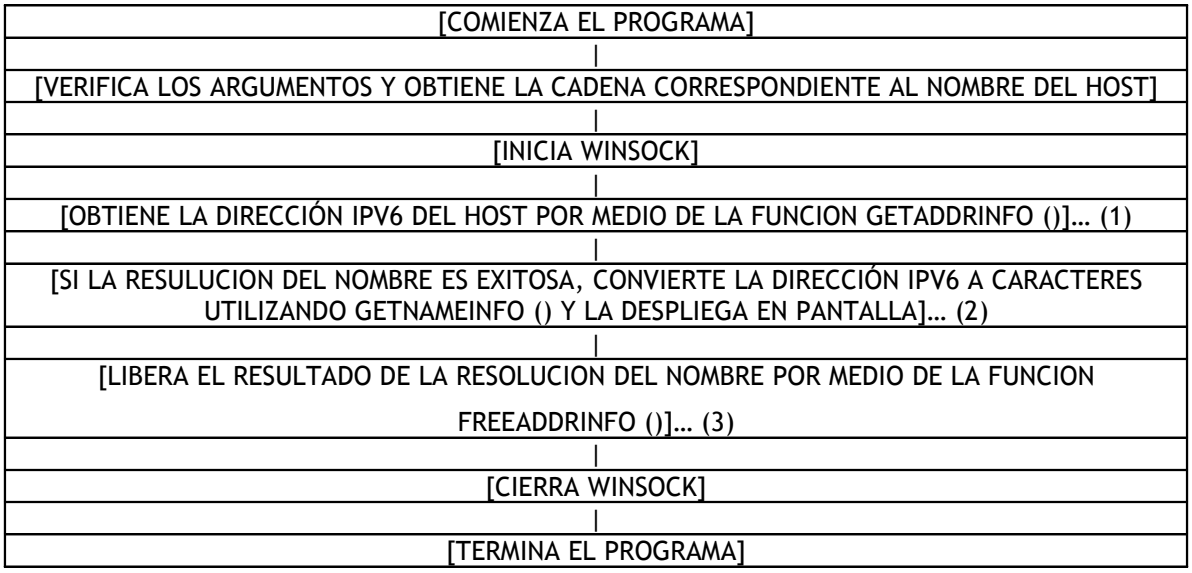


Acerca de la compilación

Una librería de importación, “ws2_32.lib”, es vinculada cuando se compila el código (getv6addr.c). Esta librería es el punto de entrada al API y siempre es necesario vincularla cuando se utiliza el API Winsock2.

Acerca del código

El flujo general del programa es el siguiente:



En el bloque (1), la función getaddrinfo () toma un nombre de host y guarda la dirección IPv6 que fue obtenida en la resolución del nombre en la estructura ADDRINFO. Si se obtienen múltiples direcciones IPv6 de dicha resolución, regresará el primer ítem (ai0) de la lista ADDRINFO. El buffer para la estructura ADDRINFO donde esta dirección IPv6 es almacenada será creado por la función getaddrinfo (). No se necesita asignarlo en el programa de antemano, sin embargo, será necesario liberarlo por medio de la función freeaddrinfo (bloque (3)) cuando ya no se necesite.

En el bloque (2), se itera a través de la estructura ADDRINFO que fue devuelta por getaddrinfo () utilizando un FOR. Para cada una, la dirección IPv6 binaria (formato binario de red) es convertida a caracteres (formato de presentación). El API que se utiliza acá es getnameinfo (). El resultado de la

conversión se almacena en v6addr. El principal rol de getnameinfo es encontrar el nombre del host de una dirección IP (reverse lookup), sin embargo, puede convertir una representación binaria a una cadena de caracteres también.

Los API utilizados en este programa, getaddrinfo (), getnameinfo (), freeaddrinfo () y gai_strerror () son importantes y pueden ser utilizados en muchos programas sin importar el sistema operativo. El RFC3493 define como usarlos. Puede haber ciertas diferencias y restricciones entre sistemas operativos.

Sobre WinSock

En el código se encuentra una variable wsaData del tipo WSADATA, y también están las funciones WSAStartup (), que se refiere a la variable, y WSACleanup (). Estas son extensiones únicas en Windows. Para WinSock, la inicialización (WSAStartup ()) y desconexión (WSACleanup ()) son siempre necesarias antes de utilizar cualquier API de los sockets.

La configuración del ambiente de desarrollo y la forma de compilación son necesarias para hacer cualquier desarrollo orientado a WinSock2 que es el que actualmente soporta la nueva tecnología de IPv6.

Para mayor información acerca del uso del WinSock2 para desarrollo de aplicaciones, referirse a:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winsock/winsock/windows_sockets_start_page_2.asp