UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES.

CAMPUS ARAGÓN

ELABORAR UNA PROPUESTA DE SEGMENTACIÓN Y ADMINISTRACIÓN PARA LA RED LAN DE LA ENEP ARAGÓN.

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A :

MARCO ANTONIO MEJÍA LARA.

ASESOR:

DR. ENRIQUE DALTABUIT GODAS. .

PAGINACIÓN

DISCONTINUA

4/1

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO
CAMPUS ARAGON
ÁREA DE INGENIERÍA EN COMPUTACIÓN

San Juan de Aragón, Edo. de Méx., a 23 de junio de 2000.

Tesis que desarrollará el (la) C.: **Marco Antonio Mejía Lara**

De la Carrera de Ingeniería en Computación

Titulo de la Tesis.

ELABORAR UNA PROPUESTA DE SEGMENTACIÓN Y ADMINISTRACIÓN PARA LA RED LAN DE LA ENEP ARAGÓN.

Capítulos:

Introducción

1. Antecedentes históricos y conceptos relacionados

2. Situación actual y análisis de la estructura de la Red de la ENEP Aragón

3. Propuesta de segmentación y redireccionamiento para la Red de la ENEP Aragón.

4. Propuesta de administración y monitoreo para la Red de la ENEP Aragón.

Conclusiones

Dr. Enrique Daltabuit Godaz
Director de Tesis

M. en C. Jesús Díaz Barriga Arceo
Jefe de Carrera

Dirección: Ed. José Villagran C #301 Col. El Rosario Tlalnepantla Estado de México. C.P. 54090

Teléfono: 53-83-28-47

Promedio: 8.88

VNIVERSIDAD NACIONAL
AVFNOMA DE
MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
ARAGON
DIRECCION

MARCO ANTONIO MEJÍA LARA
P R E S E N T E.

En contestación a la solicitud de fecha 4 de septiembre del año en curso, relativa a la autorización que se le debe conceder para que el señor profesor, Dr. ENRIQUE DALTABUIT GODAS pueda dirigirle el trabajo de tesis denominado, "ELABORAR UNA PROPUESTA DE SEGMENTACIÓN Y ADMINISTRACIÓN PARA LA RED LAN DE LA ENEP ARAGON" con fundamento en el punto 6 y siguientes, del Reglamento para Exámenes Profesionales en esta Escuela, y toda vez que la documentación presentada por usted reúne los requisitos que establece el precitado Reglamento; me permito comunicarle que ha sido aprobada su solicitud.

Aprovecho la ocasión para reiterarle mi distinguida consideración.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
San Juan de Aragón, México, 19 de septiembre del 2000
EL DIRECTOR

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGON UNAM

M en R.I. CARLOS EDUARDO LEVY VÁZQUEZ

C p Secretaría Académica.
C p Jefatura de la Carrera de Ingeniería en Computación.
C p Asesor de Tesis.

CELV/AIR/RCR/lla.

AGRADECIMIENTOS:

A Dios, por darme fuerzas en todo momento de mi vida y no dejarme flaquear.

A mis padres y hermano, por apoyarme siempre que los necesite, hacer de mi una persona honesta, dedicada y sincera. Todos mis logros también son de ustedes.

A la Universidad Nacional Autónoma de México, por forjarme como un profesionista disciplinado, responsable y capaz, por darme tanto sin recibir nada a cambio, simplemente por ser la U.N.A.M.

A Sandra, por tanto amor, comprensión, apoyo durante el tiempo que llevamos de conocernos.

A todos mi amigos y compañeros de la ENEP, con quienes he vivido momentos inolvidables.

Gracias a todos ustedes tienen un lugar muy importante en mi corazón.

DEDICATORIAS:

Dedico ésta tesis a mis Padres, Antonio Mejía Chavez, Lucina Lara de Mejía, a mi hermano Ricardo Mejía Lara, por su apoyo ininterrumpido, amor y comprensión. A Sandra Sánchez Fernández de Lara por el apoyo en este proyecto, y en todo momento. A cada una de las personas que me apoyaron durante el desarrollo de este trabajo, al Dr. Enrique Daltabuit por la paciencia y trabajo dedicados, al Ing. Marcelo Pérez Medel, por el esfuerzo y tiempo dedicados a este proyecto, A cada uno de mi revisores por tomarse el tiempo e indicarme sus puntos de vista al respecto de este trabajo.

Gracias esta tesis también es de ustedes.

INDICE

INTRODUCCIÓN.

Debido a que continuamente las redes transportan información vital para la Universidad Nacional Autónoma de México y todas su dependencias como el Campus Aragón *(Comúnmente llamada E.N.E.P. Aragón, Escuela Nacional de Estudios Profesionales Aragón, así nos referirnos al Campus Aragón de la U.N.A.M.)*, su disponibilidad y buen funcionamiento se vuelven críticos para la organización de las actividades académico – administrativas de la Institución. De igual manera, cuando se presenta algún problema con una aplicación, existen puntos de vista encontrados entre los desarrolladores y el área de administración al momento de identificar de quién es responsabilidad resolverlo.

En la adquisición o desarrollo de aplicaciones, existen un dimensionamiento para los equipos que van a soportar las nuevas aplicaciones, sin embargo, rara vez se mide la capacidad real de la red para validar si puede cubrir los nuevos requerimientos.

Por todo lo anterior, el presente trabajo tiene como objetivo encontrar la problemática en la Red de la ENEP Aragón, debido a la mala planeación a futuro y poca administración de la red; a su vez conocer las causas y consecuencias que esto conlleva, generando así una solución optima a dicha problemática; basándonos en una propuesta tecnológica y una administrativa, definidas en los dos últimos capítulos.

Para el mejor entendimiento del problema y la posible solución se ha dividido este trabajo en 4 capítulos, que son los siguientes:

Capítulo 1. Antecedentes históricos y conceptos relacionados. El objetivo de este capítulo es empaparnos de los conocimientos necesarios para la ubicación de la problemática, es decir; conocer cuál fue el crecimiento de la red y cómo se dio, así como establecer los conceptos utilizados en los posteriores capítulos.

Capítulo 2. Situación actual y análisis de la estructura de la Red de la ENEP Aragón. Este capítulo es uno de los más importantes, debido a que ayudará a conocer más a detalle los problemas existentes dentro de la Red de la ENEP Aragón. Ya que en él se mencionaran los errores en las redes locales como es una mala instalación física; de hecho, un cableado

defectuoso puede degradar e incluso "tirar" una red *(esto lo pude observar en el momento de realizar este trabajo en el Area de Posgrados).* Por lo tanto, existen equipos *(scanners)*[1] que prueban el cableado desde el conector que llega a la PC hasta la conexión con el concentrador *(hub)*, detectando importantes deficiencias. Existen infinidad de maneras de detectar los problemas en las redes, incluso no se debe descartar la simple observación y el preguntarle al usuario final su desempeño de la red durante el trabajo cotidiano, él es un buen foco de advertencia para nuestro análisis.

Capítulo 3. Propuesta de segmentación y reedireccionamiento de la Red de la ENEP Aragón. Es importante señalar que este tipo de análisis constituye una valiosa ayuda en la decisión para adquirir o actualizar equipos, así como la selección de nuevas tecnologías, evitando así compras de "pánico" o de equipos innecesarios. Yo me encargaría de proponer lo más optimo para las necesidades de la ENEP Aragón en este capítulo.

Para lograr lo anterior, es necesario tomar muestras periódicas del uso de la red como una base de comparación *(baseline)*, la cual permita medir el impacto de cambios como: la conexión de nuevos nodos, incremento en el número de usuarios, instalación de aplicaciones, etc. Y así tomar verdaderas acciones proactivas. Estas acciones las propondré en el tercer capítulo.

Capítulo 4. Propuesta de Administración y monitoreo de la Red de la ENEP Aragón. Aquí mencionaré y daré una pequeña introducción de la manera en que sería más conveniente la administración de RED de la ENEP Aragón. La administración de una Red puede incluso llevarse un trabajo completo en conceptos y metodologías, por eso solo propondré la que a mi gusto podría ser la mejor solución para la ENEP Aragón. Por ejemplo.

Es recomendable contar con equipos llamados monitores estadísticos conectados en todas las redes. La desventaja de probes[2] comerciales (monitores estadísticos), es el costo muy elevado en redes grandes ya que se necesita uno en cada red. Pero actualmente existen soluciones GNU que nos ayudarían a reducir estos gastos, además de obtener un rendimiento muy aceptable.

Los analizadores de protocolos expertos son muy útiles aunque su costo es considerable.

El uso de equipos de monitoreo estadísticos y analizadores de protocolos permite la recolección de información valiosa sobre el funcionamiento de la red; de cualquier manera, la información en sí misma no es suficiente: la interpretación y la toma de decisiones correctas es fundamental. Pero una descripción más detallada la describiré en el contenido del capítulo 4.

[1] Dispositivo físico que se conecta en forma de T a la red, para probar el estado físico del cableado.

Todo esto aunado a propuestas de creación de centros especializados para la Administración centralizada de la ENEP Aragón.

Es así como propondré una solución al mal desempeño de la Red de la ENEP Aragón, ocasionado por "colisiones", direcciones IP repetidas, falta de segmentación entre las redes, equipo en mal estado, e infinidad de problemas que se encontraron; así como una propuesta de administración y monitoreo que nos ayudará a evitar que esta problemática se presente de nuevo.

[2] Dispositivos físicos conectados en T, para "escuchar" o "simular" el tráfico en la red.

CAPITULO 1

Antecedentes históricos y conceptos relacionados.

1.1. Antecedentes históricos de RedUNAM y la red de la ENEP Aragón.

A finales de la década de los 60's y principios de los 70's se instaló en Ciudad Universitaria una red telefónica de cobre, la cual sirvió como medio de comunicación entre teletipos y una computadora central, formando así el inicio de la red universitaria que después conoceríamos como RedUNAM[3].

La RedUNAM es un sistema de transmisión de datos entre las facultades, institutos, centros de difusión, coordinaciones y demás dependencias de la UNAM. En resumen es la red universitaria de telecomunicaciones.

Manejando la tecnología de cobre empieza a difundirse por toda la Universidad esta red, contemplando en un principio servicios que iban desde terminales de caracteres, de graficación e impresión hasta interconexión con estaciones de trabajo, todas conectadas remotamente utilizando líneas telefónicas. De esta manera continúa creciendo esta infraestructura así como las necesidades de los usuarios, por lo que la UNAM se volvió el segundo nodo de Internet en México, más específicamente el Instituto de Astronomía en la Ciudad Universitaria. A través de una conexión vía satélite de 56 kbps

En la ENEP Aragón el proceso fue lento; el surgimiento del Centro de Cómputo a finales de los 70's fue el comienzo, en donde los primeros equipos no estaban conectados a una red de telecomunicaciones pero con el paso del tiempo se agregaron a una, siendo el comienzo de la integración de la ENEP Aragón a RedUNAM. Podemos contar que al principio el Centro de Cómputo del Campus Aragón[4] (C.C.C.A) tenia a su cargo una máquina eclipse y 6 máquinas perforadoras, el procedimiento para el desarrollo de un programa era muy lento debido a que

[3] Fuente: http://www.nic.unam.mx/redunam/historia.html.
[4] C.C.C.A. = Centro de Computo del Campus Áragon.

solamente se podía utilizar el equipo en dos o máximo tres ocasiones en el día, aparte de que se tenía que reservar tiempo de perforadoras para realizar cualquier programa, ya perforadas las tarjetas del programa, se entregaban para ser compilados en una de las sesiones diarias de la eclipse junto con todos los demás programas del día, y luego esperar bastante tiempo que iba de 6 horas hasta en ocasiones un día completo para recibir los resultados, esto era muy engorroso sin embargo fue el principio.

En octubre de 1987 la UNAM se conecta a BITNET, directamente al Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM) campus Monterrey, usando unas líneas analógicas de 9600 bps. Esta Universidad se conectaba a San Antonio Texas específicamente a la Escuela de Medicina de la Universidad de Texas, la cual también era una línea analógica de 4 hilos a 9600 bits por segundo.

Mientras tanto en Áragon, á finales de los 80's llega a la ENEP, Omninet. La primera red que se instaló en un pequeño salón del C.C.C.A.; la cual era una red conectada a través de cable telefónico. Esta red estaba limitada en funciones ya que solo permitía la transferencia de archivos. La segunda fue Arnet, una red más robusta, la cual contenía un servidor de archivos y de impresión bajo Sistema Operativo Novell[5].

Para consolidar estos avances dentro de la red BITNET la UNAM empezó a utilizar la computadora IBM 4381 como servidor de correo electrónico y otros servicios de esta red. Durante este proceso se comenzó a instalar terminales IBM.

Continuando con este crecimiento se establece un enlace con la SCT[6] a su red TELEPAC, para un proyecto que nunca se llevo a cabo; hasta 1989, otra vez, por medio del Instituto de Astronomía se enlaza a las red NFS[7] de EUA por medio del satélite mexicano Morelos II.

Con el paso del tiempo fue creciendo la red en la UNAM, dando algunos pasos importantes como; conectar la red LAN del Instituto de Astronomía con la DGSCA utilizando enlaces de fibra óptica. Esto dio inicio a una revolución en las comunicaciones dentro de la UNAM, la adquisición masiva de equipo de cómputo que rápidamente se fue integrando a redes locales y éstas a su vez empezaron a comunicarse entre si, los enlaces satelitales a Cuernavaca, Morelos, y a San Pedro Mártir en Ensenada, los enlaces de Microondas dentro de las escuelas y dependencias en la Ciudad de México. Todo esto fue la punta de lanza para establecer la Dirección de

[5] Fuente: http://www.aragon.unam.mx/historia.htm
[6] SCT = Secretaria de Comunicaciones y Transportes.
[7] Red del Centro Nacional de Investigación Atmosférica (NCAR) de Boulder, Colorado, en los E.E.U.U.

Telecomunicaciones Digitales en la DGSCA[8], la cual tenía como principal tarea la creación de la Red Integral de Telecomunicaciones de la UNAM, ésta debería ser capaz de poder transmitir voz y datos a través de todas las dependencias de la Universidad no importando su ubicación geográfica.

En 1990 debido a la creciente necesidad de mantener en buen estado esta naciente Red de Telecomunicaciones, así como poder integrar los servicios y recursos de cómputo para los que fue implementada *(investigación y docencia)*, se crea el Laboratorio de RedUNAM, Las principales funciones de este centro son: la investigación, el estudio, el análisis de las comunicaciones, el análisis de las topologías de redes, el análisis de los protocolos y por supuesto los servicios a la comunidad universitaria. Oficialmente la Red Integral de Comunicaciones y Telecomunicaciones fue inaugurada en 1992.

Pero no solo en el C.C.C.A. fue instalada una red, también en el departamento de Informática, en el Centro de Lenguas, el edificio de Gobierno y Biblioteca se instalaron redes con servidores con Sistema Operativo Novell, como servidores de archivos y de impresión con cable coaxial; éstas fueron las tecnologías utilizadas en esos tiempos para la comunicación y transferencia de archivos. Debido a que en su momento este tipo de tecnologías eran las más usadas en el mundo.

Al principio todas las redes de la ENEP Aragón estaban separadas y el departamento de informática era el encargado de mantener una administración muy rústica en ellas excepto en la del C.C.C.A. Durante este tiempo (finales de los 80's) es cuando se agrega la red de Posgrado conectándose desde Informática, también utilizando cable coaxial, Novell y un repetidor. Ésta red fue uno de los puntos más conflictivos de la administración debido al mal estado del cable coaxial utilizado, durante el levantamiento de la información de este proyecto.

Durante 1986 el crecimiento del C.C.C.A. fue tal que se tubo que cambiar la ubicación de éste, incrementando en tres veces su tamaño. Durante este periodo se empezó a comprar equipo que facilitaba el trabajo de los usuarios, dentro de los cuales destaca la máquina HP 1000, con 31 terminales, 2 equipos Onyx con 10 terminales cada una y 6 microcomputadoras. Así estuvieron disponibles las primeras redes para la ENEP Aragón, y el protocolo utilizado fue TCP/IP.

Á mediados de los 90's se hicieron los primeros intentos por conectarse a C.U. mediante microondas, mientras que las conexiones en cada una de las redes fueron mediante cable coaxial.

[8] Dirección General de Servicios de Computó Académico.

Con el paso del tiempo siguió creciendo y llegando equipo necesario para el buen funcionamiento del las tareas encomendadas al C.C.C.A. llegando a la ENEP la U6000 y la HP9000 que posteriormente se unieron mediante una red de cable coaxial. Los equipos Unisys fueron las primeras PC's conectadas también con coaxial a la red del C.C.C.A.

Aquí comienza un cambio importante en las redes de la ENEP; ya que fue necesario unir las diferentes redes de la ENEP y la fibra óptica fue el medio por el cual se hizo esta unión. A su vez el edificio de Gobierno estaba siendo remodelado y se apreovecha para cambiar el cable coaxial por UTP (par trenzado) en las mayoría de las redes de la ENEP, es decir en el C.C.C.A., en la Biblioteca y por supuesto el edificio de Gobierno, exceptuando la del centro de lenguas que fue eliminada por considerarse innecesaria; también durante estos cambios se aprovecha para instalar redes de UTP en A504, laboratorios y Fundación UNAM, poco después el Centro Tecnológico se agrega a esta infraestructura.

Podemos concluir entonces que el primer sistema operativo propiamente de red que se instaló en la ENEP Aragón fue Novell, y por consiguiente también la primera red Ethernet, para entonces los enlaces a C.U. estaban muy avanzados y a mediados de los 90's la ahora unificada red de la ENEP Aragón se conecta con RedUNAM, formado así parte de la Red de Telecomunicaciones de la U.N.A.M.

1.2. Servicios proporcionados por RedUNAM y la red de la ENEP Aragón.

La RedUNAM / Internet nos ofrece gran cantidad de servicios a toda la comunidad universitaria; administrativos, investigadores, profesores y alumnos en general. Pero sin lugar a duda los más populares han sido el WWW, correo electrónico y la transferencia de archivos mediante FTP. Estos son por supuesto los servicios que el usuarios debe conocer para mantenerse en contacto por medio de esta inmensa red universitaria, así como para poder manejar grandes volúmenes de información. Solo por nombrar algunos datos, la UNAM cuenta con más de 15 mil equipos de cómputo conectados a la red de redes[9], aparte de brindar servicio a otras instituciones para que se conecten a Internet por medio de RedUNAM, lo que suma anualmente más de 8 mil equipos de cómputo adicionales.

Podemos clasificar de manera muy general en dos tipos a las computadoras que integran a la RedUNAM: Las que nos brindan servicios de información que conocemos como "servidores" y las que accesan a estos datos llamadas "clientes". Los servidores dependiendo para que aplicaciones estén destinados tienen muchas características, pero la que todos ellos tienen en común es que

[9] Fuente: http://www.dgsca.unam.mx/

los "servidores" tienen conexiones permanentes a la red y brindan sus servicios todo el año a cualquier hora; los "clientes" por su parte pueden estar conectados de muchas maneras que van de esta forma con conexiones permanentes hasta los enlaces por líneas telefónicas conmutadas es decir, vía módem.

La RedUNAM al formar parte integral de Internet ofrece todos los servicios propios de esta red mundial además de los propios de una red institucional, inclusive como ISP (Internet Service Provider) para alumnos, Investigadores e inclusive otras instituciones educativas o gubernamentales.

El Correo electrónico como mencionamos anteriormente es una de las herramientas más utilizadas en estos tiempos, pero ¿qué es esta tecnología y cómo funciona?. El correo electrónico no es muy diferente del correo común y corriente, pero con muchas ventajas entre las que destacan su rapidez y economía, en el correo tradicional nosotros necesitamos un lugar en donde nos va a llegar nuestra carta, es decir un buzón o apartado postal en donde se almacenarán los correos en espera de ser leídos, de igual manera en el correo electrónico, esta función la realiza el servidor de correo electrónico, existen infinidad de programas servidor como Sendmail, Qmail, PostOffice, entre otros. Este servidor es nuestro buzón. También se necesita un software "cliente" para que ya conectados a nuestra oficina postal podamos leer nuestro correo. Con el correo electrónico podemos mantener comunicación tanto con usuarios internos de la RedUNAM como externos que pueden ser nacionales o internacionales, todo a través de la Red Internet y una dirección única de buzón que no es otra cosa que la clave de usuario (login) y el Host al que pertenece este usuario unidos por un carácter especial, la arroba (@).

Tanto en el correo electrónico como en el correo tradicional tenemos que mantener un cierto orden en nuestro envió de mensajes, es decir un formato especfico para poder garantizar la entrega correcta de nuestro mensaje. Este formato consta principalmente de 3 partes; encabezado, cuerpo y attachment. En nuestra carta ordinaria y electrónica las partes de un encabezado son:

Ordinaria:

- Remitente. (De): Nombre.
  Dirección.
- Destinatario. (Para): Nombre.
  Dirección.
- Asunto:

De la misma manera la carta electrónica tiene estas partes con algunos campos extras.

- TO: (Destinatario; Nombre y Dirección)
- FROM: (Remitente; Nombre y Dirección)
- SUBJECT: (Asunto)
- CC: (Con copia para)
- BCC: (Con copia ciega para)

La segunda parte en ambas es el cuerpo de nuestra carta, que no es otra cosa que la carta propiamente, es decir el mensaje que queremos trasmitir, en la carta electrónica comúnmente llamado "Body". Nosotros en nuestros clientes encontraremos el body como un espacio en donde podemos escribir el texto del mensaje, en otras palabras es nuestro "papel" en donde escribiremos.

En ocasiones, nosotros queremos enviar adjunto a nuestra carta algún paquete al que se le debe tener ciertos cuidados especiales para que no se dañe. En el correo electrónico no hay que preocuparse por esto lo podemos hacer mediante los archivos adjuntos usualmente llamados "Attachments". Estas son las tres partes importantes de un correo ya sea electrónico o normal, en ocasiones estas partes pueden ser un poco modificadas e incluso el "attachment" puede ser parte del "body" o del "header" dependiendo del "cliente" de correo que se este usando.

La transferencia de archivos mejor conocido como FTP es otro de los servicios más usados dentro de la RedUNAM. El FTP es el envió de archivos a través de la red, usted puede decir que esto ya se hacia antes de la llegada de Internet por medio de disquetes o cintas magnéticas o algún otro medio de almacenamiento de archivos, pero imagínese ahora el tamaño de los archivos de hoy en día y lo engorroso que resultaría utilizar estos dispositivos para la trasferencia de archivos ya que su fin precisamente no fue la transferencia si no el almacenamiento de archivos, además de que no podríamos poner a disposición del público en general esta información tan fácilmente. Y es aquí en donde el servicio de "FTP anónimo" nos da una de sus tantas ventajas. La mejor manera de comprender este servicio es a través de la comparación con una biblioteca pública; existen diferentes colecciones de archivos en bibliotecas electrónicas (servidores FTP) que brindan este servicio al público en general, estos sitios tienen una gran cantidad de información y muy frecuentemente especializada en algún tema o área en especifico, es decir podemos encontrar en Internet y RedUNAM sitios FTP anónimos dedicados a productos comerciales, diseño, vacunas, lenguajes de programación, etc. Esto es por lo general para lo que se emplea este servicio, para la obtención de utilerías diversas, aunque no se descarta el simple envió de archivos por separado como: imágenes, documentos, audio, etc.

Sin lugar a dudas el servicio más popular y que ha dado un gran impulso al uso de nuestra red es el servicio del World Wide Web, www o mejor conocido como el "web". Este servicio también es el servicio más popular de la Internet, el cual basa su funcionamiento en el Hiper-Texto un concepto relacionado al manejo de documentos a través de enlaces o ligas a diferentes partes del documento o inclusive imágenes, vídeo y audio.

Fue en marzo de 1989, cuando dos investigadores del Laboratorio Europeo de Física de Partículas, Tim Berners-Lee y Robert Cailliau, mostraron la idea de un sistema distribuido que resolvía el problema de extravío de información, además de permitir el acceso e intercambio de datos a colegas por toda Europa, dando como resultado la concentración en un solo lugar de la información.

Actualmente nosotros podemos observar infinidad de "páginas web" en Internet con tan solo escribir el URL (Uniform Resource Locators, Localizador Uniforme de Recursos) en nuestro Browser y con ayuda a la ligas podemos "navegar" a través de este servicio de Internet. Este URL es un protocolo que ayuda a definir la sintaxis para obtener la información de los "servidores web", este protocolo consta de dos partes el URI (Universal Resorce Identifier, Identificador Universal de Recursos), y la dirección de la máquina a la cual queremos accesar; el URI es la definición del protocolo a usar como el HTTP, FTP, HTTPS, o algún otro. Por ejemplo un URL completo quedaría:

http://www.unam.mx/inscripciones/index.html

en donde http es el URI, en este caso utilizaremos el Hiper Text Transfer Protocol.

www.unam.mx es la máquina a la cual accesaremos y inscripciones/index.html es la ruta completa de un archivo dentro de la máquina.

Sabiendo esto y teniendo en cuenta la cantidad de información disponible a través de este servicio sólo tenemos que tener un Navegador (Browser) para poder hacer uso de ella. Los más utilizados sólo por mencionar algunos son: el Netscape Navigator y el Explorer de Microsoft.

1.3. Conceptos generales.

Concepto de red; La definición más simple y también la más aceptada es la siguiente: una red es un conjunto de computadoras conectadas entres si (ocasionalmente terminales) mediante uno o varios medios de transmisión guiados o no guiados que pueden ser la línea telefónica, cable

coaxial, fibra óptica, satélites, infrarrojos, etc. El principal objetivo de una red es la transmisión e intercambio de datos entre estas computadoras o terminales.

Las redes de computadoras proporcionan muchas ***ventajas***, principalmente:

1. Proporcionan la posibilidad de que la información pueda estar disponible en cualquier punto de la red, incluso si se encuentra en una diferente ciudad.
2. Existe la posibilidad de compartir recursos, es decir, podemos distribuir nuestro trabajo entre las diferentes terminales o servidores de la red. Por ejemplo alguna impresión, o algún proceso.
3. Teniendo en cuenta lo anterior, un sistema de red se puede volver un gran soporte para fallas en caso de alguna emergencia. Por ejemplo una computadora puede fallar y ser parte medular en nuestra producción, alguna otra puede tomar su lugar en un lapso corto de tiempo; claro dependiendo del sistema que este monitoreando y nuestra visión para prevenir desastres.
4. Flexibilidad es otra de las ventajas, nos referimos al caso de poder conectarnos a la red desde cualquier lugar incluso desde nuestra casa con tan solo un modem, facilitando así nuestro trabajo. Imaginémonos que estamos en viaje de negocios y necesitamos recibir archivos importante de nuestra empresa como estadísticas de ventas, tan solo nos conectamos a un servidor con la información necesaria como puede ser el caso de una extranet por ejemplo.

El modelo de referencia OSI

El modelo OSI (Open Systems Interconnection) fué desarrollado por el ISO (Organización Internacional de Normalización) para establecer una estructura común dentro de las redes de comunicación, dividiendo el conjunto de tareas de comunicación en siete niveles.

El modelo permite que cada nivel se ocupe de unas tareas y utilice los servicios de niveles inferiores sin necesidad de preocuparse de cómo funcionan, asegurando una compatibilidad entre máquinas a cada nivel.

Se pueden dividir los niveles en dos grupos:

Servicios de soporte al usuario (niveles 7, 6 y 5).
Servicios de transporte (niveles 4, 3, 2 y 1).

Descripción de niveles OSI

Nivel 7, aplicación: se encarga de proporcionar un entendimiento entre usuarios de distintos equipos, sin importar el medio ni el protocolo empleado. Es decir, establece un tema de diálogo.
Nivel 6, presentación: facilita la comunicación a nivel de lenguaje entre el usuario y la máquina que esté empleando para acceder a la red.
Nivel 5, sesión: establece el control de comunicación, indicando quien debe transmitir o recibir, además de señalar el inicio y fin de la sesión de comunicación.
Nivel 4, transporte: establece el medio de comunicación, asegurando la transferencia de información sin errores en ambos sentidos.
Nivel 3, red: se encarga del encaminamiento de mensajes entre nodo y nodo, a través de un medio físico, sin importar el contenido del mensaje.
Nivel 2, enlace: mantiene la comunicación entre cada par de nodos de la red, apoyándose en un medio físico de conexión.
Nivel 1, físico: establece los medios materiales para efectuar el enlace entre nodos (conectores, cables, niveles de tensión, etc).[10]

La figura 1 muestra la estructura del modelo OSI, descrito anteriormente.

Fig. 1 Capas del Modelo OSI

Redes de área local (LAN) : son de cobertura pequeña , velocidades de transmisión muy elevadas , utilizan redes de difusión en vez de conmutación , no hay nodos intermedios .

*Una **LAN** es un sistema que permite conectar directamente varias estaciones entre si. Es un* sistema por que implica que va haber componentes de hardware y software, va a conectar por que

[10] Fuente: MCSE TCP/IP Exam Cram, Gari Novosel

queremos que las terminales transmitan información entre ellas, y directamente, por que no se comunica una terminal con otra terminal de una red diferente si no se comunica con terminales dentro de la misma red. Para que los terminales se comuniquen directamente se tendría que:

- Utilizar un cable para comunicar un terminal con todos los demás.
- Utilizar un solo cable (un solo medio de transmisión) y los terminales están conectados a este cable.
- Utilizar un dispositivo que conecte todas las estaciones, el dispositivo puede ser un Hub o Switch.

Al haber varias estaciones deberemos tener un sistema de direcciones que identifiquen las estaciones. Estas direcciones son: MAC, física (id de la estación dentro de una red), hardware.

La dirección más importante es la de acceso al medio (MAC) que es la que permite llegar a la estación.

Tiene que haber una topología o forma de conexión entre los diferentes terminales.Las LAN's se comunican con la filosofía *red broadcast* o *por difusión*. En esta filosofía una trama es vista por todas las demás estaciones y se copiará en la estación en que tenga el identificador igual que el identificador destino de la trama. Las LAN necesitan un algoritmo de acceso al medio, ya que podría pasar que todos los terminales quisieran transmitir al mismo tiempo y de esta forma se produciría una colisión, por lo tanto se ha de controlar el acceso al medio.

Resumiendo tenemos las siguientes características:

- Esta conexión utiliza un medio (cable, infrarrojos, ondas, etc.) compartido por todos las computadoras
- Tienen que formar una topología (conexión en bus, en forma de anillo, estrella, etc.). Estas dos características definen el nivel físico.

- Necesitaremos un algoritmo de arbitraje (acceso al medio) además de las funciones vistas anteriormente. La figura 2 muestra la arquitectura física de una red LAN.

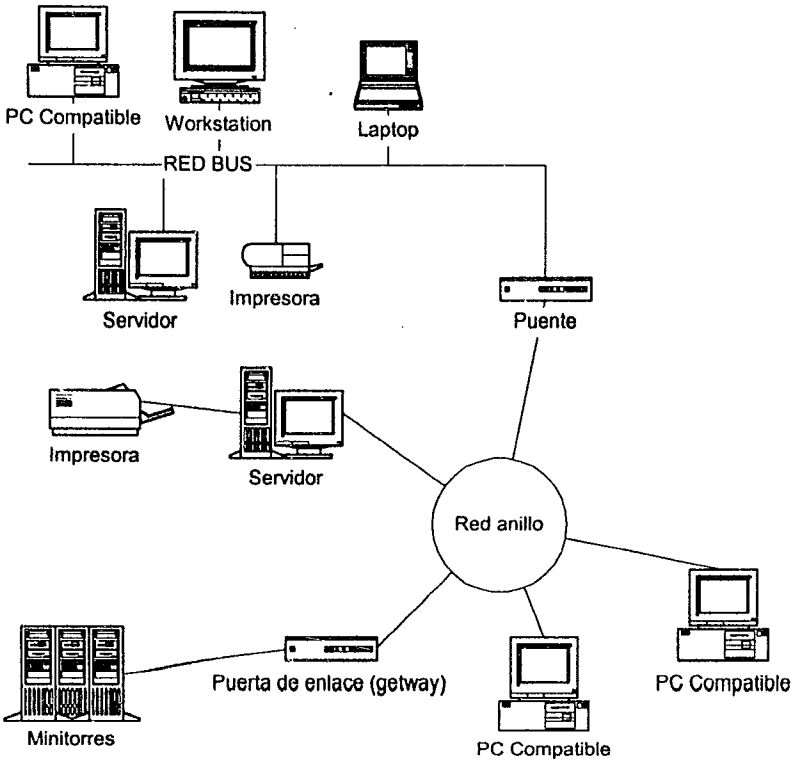


Fig. 2. Arquitectura física de una Red LAN

Redes de área amplia (WAN) : Son todas aquellas que cubren una extensa área geográfica Son generalmente una serie de dispositivos de conmutación interconectados. Se desarrollan o bien utilizando tecnología de conmutación de circuitos o conmutación de paquetes.

Se utiliza un medio muy rápido para la comunicación, pero solo tenemos un medio. Por lo tato los ordenadores están conectados a un aparato que multiplexa y envía la información y busca rutas. Por lo anterior estas redes generalmente son de velocidades más bajas y son usadas para conectarse a las redes LAN por las empresas. Por ejemplo una WAN comúnmente utiliza lineas telefónicas dedicadas con capacidad de transmitir datos a velocidades de 56 kilobits/seg o 1.55 megabits/seg, y con ellas podemos conectar oficinas en distintos puntos de una ciudad o incluso al otro lado del mundo.

El funcionamiento de una WAN puede causar confusiones pero en realidad es sencillo. Las WAN se componen de diferentes nodos, estos nodos son equipos que interconexionan estaciones o sirven de intermediario para la comunicación entre los diferentes terminales conectados a la WAN.

Los terminales se conectan al nodo de acceso, los cuales se conectaran al resto de nodos. A los nodos se pueden conectar otras WAN o LAN. La figura siguiente muestra un diagrama de esté tipo de red.

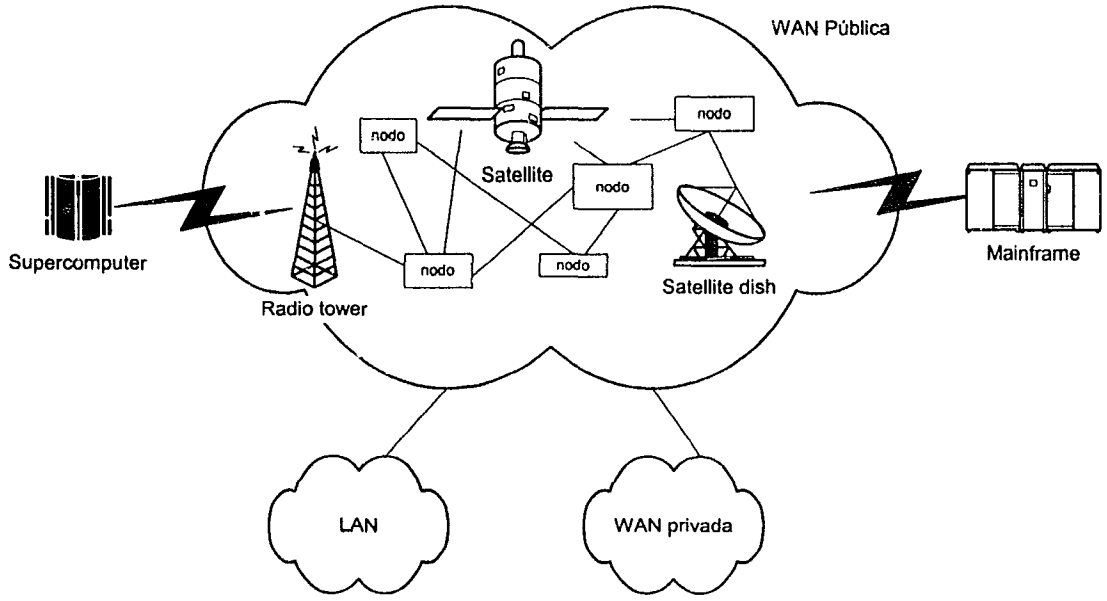


Fig. 3 Arquitectura de una Red WAN

Topologías.

Una topología es la distribución física de las estaciones de trabajo, computadoras, impresoras y demás dispositivos, así como los cables y medios que las conectan entre sí.

Las estaciones de trabajo de una red se comunican entre sí mediante una conexión física (el medio de transmisión) y el objetivo de la topología es buscar la forma más económica y eficaz de conectarlas para, al mismo tiempo, facilitar la fiabilidad del sistema, y evitar retrasos en la transmisión de datos, permitir un mejor control en la red y permitir en forma eficiente el aumento en de las estaciones de trabajo.

Las formas más utilizadas son:

Configuración en bus. Todas las estaciones de trabajo comparten el mismo canal de comunicaciones, por ese mismo canal circula la información y cada estación recoge la información que le corresponde.

Esta configuración tiene muchas ventajas; es fácil de instalar, se utiliza el mínimo de cable, fácilmente se pueden agregar o eliminar nodos en la red, la mayoría de las fallas de una estación conectada a la red no repercuten en el funcionamiento de la misma, aun si el cable que la conecta a la red tuviera una ruptura.

Pero entre sus inconvenientes destacan; es fácil de que un usuario externo se adentre sin perturbar el funcionamiento de la red, quedando así oculto, la longitud de los cable no puede sobrepasar los 2,000 metros, a menos que se utilicen otros dispositivos, el crecimiento mal planeado de la misma puede a dañar su rendimiento debido a que solo existe un solo canal de comunicación, la desventaja más significativa es que cuando el cable que funciona como bus se rompe toda la red puede ser afectada por lo que la comunicación en toda la red es interrumpida. Además encontrar el problema puede ser una tarea muy laboriosa.

A principios de los 90's fue la configuración más utilizada en el mundo y en conjunto con el tipo de red Ethernet fue la configuración más utilizada en la red de la ENEP Aragón. Esta configuración se muestra en la figura cuatro.

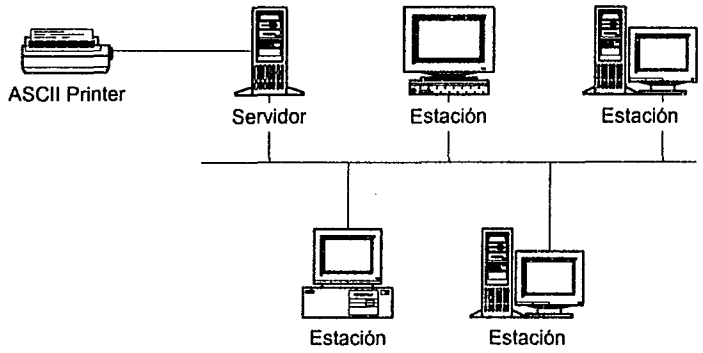


Fig 4. Topología tipo Bus

Configuración en anillo. Aquí todas las estaciones están conectadas en círculo formando un anillo, de tal forma que cada estación solo tiene contacto con dos máquinas.

El flujo de la información va recorriendo todas las terminales hasta llegar a su destino. Por lo que un inconveniente es que si la red es extensa puede llegar a ser muy lenta, pero a pesar de esto, esa lentitud no es su mayor problema debido actualmente los medios de trasporte son muy rápidos por si solos, pero su mayor problema es que si una estación falla puede llegar tirar toda la

red, más aun si el cable de comunicación se encuentra roto es muy difícil encontrar el problema y puede bloquear en su totalidad la red.

Su instalación es compleja y su uso está extendido por el entorno industrial. Es usada por la red de tipo Token Ring de IBM. La siguiente figura muestra un esquema de este tipo de configuración.

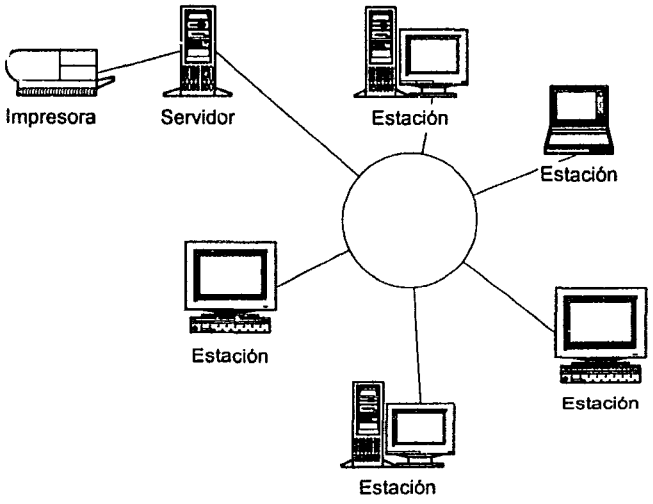


Fig. 5. Topología tipo anillo

Configuración en estrella. Está configuración es la más antigua, en ella todas las estaciones se conectan directamente al servidor o computador central, es decir todas las comunicaciones se hacen a través de él. Nos muestra la ventaja que si sucede una falla en alguna estación de trabajo no repercutirá en la red, sin embargo si esta falla se presenta en el servidor toda la red se vendrá a bajo.

Tiene un tiempo de respuesta rápido en la comunicación entre las estaciones de trabajo y el servidor pero un tiempo de respuesta lento entre una estación y otra. Su costo es caro y no muy conveniente en instalaciones grandes por la tecnología utilizada. Es usada por el tipo de red Starlan de AT&T ó SneT. [11]. La figura 5 muestra la arquitectura de este tipo de red.

[11] Fuente: http://www.cisco.com/

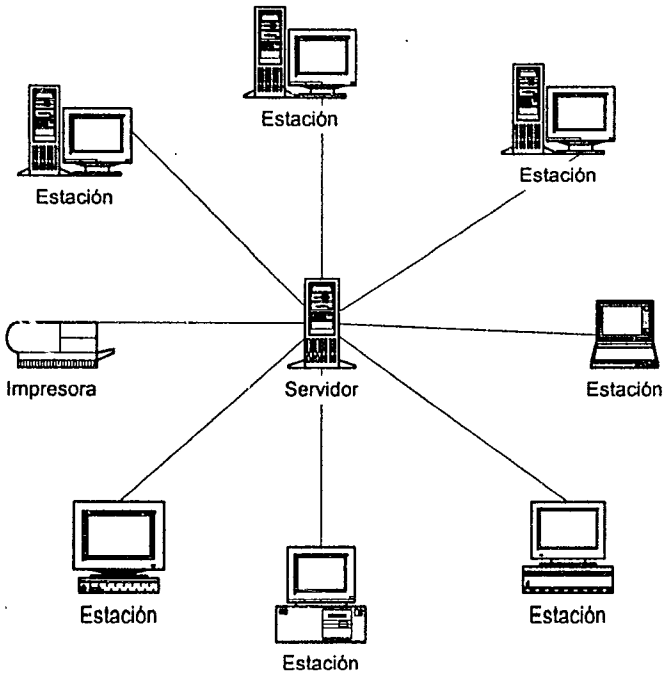


Fig. 5 Topología tipo Estrella.

Topología física y lógica.

En las configuraciones anteriores podemos notar que nos basamos para su agrupamiento en la forma en que está extendido el cableado. En otras palabras, estas configuraciones son topologías físicas. Además de este concepto de agrupamiento de terminales, en que cada red se designa una topología lógica, que describe la red desde la perspectiva de las señales que viajan a través de ella.

Un diseño de red puede tener distinta topología física y lógica, es decir la forma en que está cableada no necesariamente es la forma en que viajan los datos. Observe la siguiente figura.

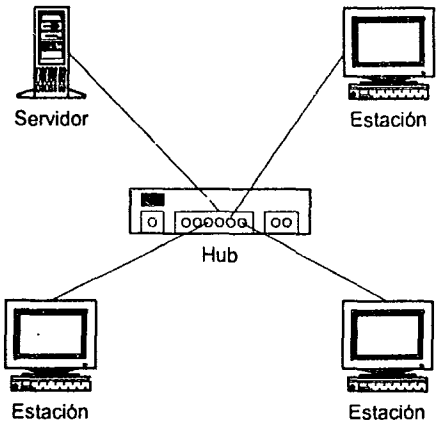


Fig. 6 Distribución de una red

En la actualidad por lo regular sucede así, todas las estaciones de trabajo están conectadas a un concentrador (HUB) simulando una configuración tipo estrella, pero dentro de este las señales se mezclan y son retransmitidas a todas las estaciones de trabajo, como en una topología tipo bus. Lo que nos da que tenemos una topología física de tipo estrella y una topología lógica tipo bus, podemos observar que en la ENEP Aragón tenemos este caso.

Medios de transmisión.

Para transportar el flujo de los datos de una máquina a otra, es necesario contar con lugar por donde pasen seguros estos datos, en redes los conocemos como medios de transmisión y los separamos en medios de transmisión guiados y en medios de transmisión no guiados.

Medios de transmisión guiados. En medios guiados, el ancho de banda o velocidad de transmisión dependen de la distancia y de si el enlace es punto a punto o multipunto.

Par trenzado

Es el medio guiado más barato y el más usado. Consiste en un par de cables, embutidos para su aislamiento, para cada enlace de comunicación. Para evitar el ruido ocasionado por el ambiente y entre los pares, estos se trenzan entre pares que contienen los mismos colores. La utilización del trenzado tiende a disminuir la interferencia electromagnética.

Su inconveniente principal es su poca velocidad de transmisión y su corta distancia de alcance. Con estos cables, se pueden transmitir señales analógicas o digitales. Es un medio muy susceptible a ruido y a interferencias. Para evitar estos problemas se suele trenzar el cable con

distintos pasos de torsión y se suele recubrir con una malla externa para evitar las interferencias externas.

Pares trenzados apantallados y sin apantallar

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

Cable coaxial

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

Se suele utilizar para televisión, telefonía a larga distancia, redes de área local, conexión de periféricos a corta distancia, etc. Se utiliza para transmitir señales analógicas o digitales. Sus inconvenientes principales son : atenuación, ruido térmico, ruido de intermodulación. Para señales analógicas, se necesita un amplificador cada pocos kilómetros y para señales digitales un repetidor cada kilómetro.

Fibra óptica

Se trata de un medio muy flexible y muy fino que conduce energía de naturaleza óptica. Su forma es cilíndrica con tres secciones radiales: núcleo, revestimiento y cubierta. El núcleo está formado por una o varias fibras muy finas de cristal o plástico. Cada fibra está rodeada por su propio revestimiento que es un cristal o plástico con diferentes propiedades ópticas distintas a las del núcleo. Alrededor de este conglomerado está la cubierta (constituida de material plástico o similar) que se encarga de aislar el contenido de aplastamientos, abrasiones, humedad, etc.

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

- Permite mayor ancho de banda.

- Menor tamaño y peso.
- Menor atenuación.
- Aislamiento electromagnético.
- Mayor separación entre repetidores.

Su rango de frecuencias es todo el espectro visible y parte del infrarrojo. El método de transmisión es: los rayos de luz inciden con una gama de ángulos diferentes posibles en el núcleo del cable, entonces sólo una gama de ángulos conseguirán reflejarse en la capa que recubre el núcleo. Son precisamente esos rayos que inciden en un cierto rango de ángulos los que irán rebotando a lo largo del cable hasta llegar a su destino. A este tipo de propagación se le llama multimodal. Si se reduce el radio del núcleo, el rango de ángulos disminuye hasta que sólo sea posible la transmisión de un rayo, el rayo axial, y a este método de transmisión se le llama monomodal.

Los inconvenientes del modo multimodal es que debido a que dependiendo al ángulo de incidencia de los rayos, estos tomarán caminos diferentes y tardarán más o menos tiempo en llegar al destino, con lo que se puede producir una distorsión (rayos que salen antes pueden llegar después), con lo que se limita la velocidad de transmisión posible.

Hay un tercer modo de transmisión que es un paso intermedio entre los anteriormente comentados y que consiste en cambiar el índice de refracción del núcleo. A este modo se le llama multimodo de índice gradual. Los emisores de luz utilizados son: LED (de bajo costo, con utilización en un amplio rango de temperaturas y con larga vida media) y ILD (más caro, pero más eficaz y permite una mayor velocidad de transmisión).

Medios no guiados. Se utilizan medios no guiados, principalmente el aire. Se radia energía electromagnética por medio de una antena y luego se recibe esta energía con otra antena.

Hay dos configuraciones para la emisión y recepción de esta energía: direccional y omnidireccional. En la direccional, toda la energía se concentra en un haz que es emitido en una cierta dirección, por lo que tanto el emisor como el receptor deben estar alineados. En el método omnidireccional, la energía es dispersada en múltiples direcciones, por lo que varias antenas pueden captarla. Cuanto mayor es la frecuencia de la señal a transmitir, más factible es la transmisión unidireccional .

Por tanto, para enlaces punto a punto se suelen utilizar microondas (altas frecuencias). Para enlaces con varios receptores posibles se utilizan las ondas de radio (bajas frecuencias). Los infrarrojos se utilizan para transmisiones a muy corta distancia (en una misma habitación).

Microondas terrestres

Suelen utilizarse antenas parabólicas. Para conexionas a larga distancia, se utilizan conexiones intermedias punto a punto entre antenas parabólicas.

Se suelen utilizar en sustitución del cable coaxial o las fibras ópticas ya que se necesitan menos repetidores y amplificadores, aunque se necesitan antenas alineadas. Se usan para transmisión de televisión y voz.

La principal causa de pérdidas es la atenuación debido a que las pérdidas aumentan con el cuadrado de la distancia (con cable coaxial y par trenzado son logarítmicas). La atenuación aumenta con las lluvias.

Las interferencias es otro inconveniente de las microondas ya que al proliferar estos sistemas, puede haber más solapamientos de señales.

Microondas por satélite

El satélite recibe las señales y las amplifica o retransmite en la dirección adecuada. Para mantener la alineación del satélite con los receptores y emisores de la tierra, el satélite debe ser geoestacionario. Se suele utilizar este sistema para:

- Difusión de televisión .
- Transmisión telefónica a larga distancia .
- Redes privadas .

El rango de frecuencias para la recepción del satélite debe ser diferente del rango al que este emite, para que no haya interferencias entre las señales que ascienden y las que descienden.

Debido a que la señal tarda un pequeño intervalo de tiempo desde que sale del emisor en la Tierra hasta que es devuelta al receptor o receptores, ha de tenerse cuidado con el control de errores y de flujo de la señal. Las diferencias entre las ondas de radio y las microondas son:

- Las microondas son unidireccionales y las ondas de radio omnidireccionales .
- Las microondas son más sensibles a la atenuación producida por la lluvia .
- En las ondas de radio, al poder reflejarse estas ondas en el mar u otros objetos, pueden aparecer múltiples señales "hermanas".

Infrarrojos

Los emisores y receptores de infrarrojos deben estar alineados o bien estar en línea tras la posible reflexión de rayo en superficies como las paredes. En infrarrojos no existen problemas de seguridad ni de interferencias ya que estos rayos no pueden atravesar los objetos (paredes por ejemplo). Tampoco es necesario permiso para su utilización (en microondas y ondas de radio si es necesario un permiso para asignar una frecuencia de uso).

Tipos de redes locales.

Hay muchos tipos distintos de redes, dependiendo del cableado, de la topología utilizada, de la forma en la que accesa al medio e incluso los protocolos utilizados. El conjunto de estos factores van a determinar la Arquitectura de la red local. Sin embargo existen estándares y tipos que son utilizadas en la mayoría de los casos, esos estándares son:

- Ethernet.
- Token Ring.
- Arcnet.

Ethernet

Esta arquitectura fue creada por Xerox Corporation y así poder enlazar un grupo de microcomputadoras, en sus laboratorios de Palo Alto en California. Se diseño para transmitir archivos y compartir periféricos.

En un principio fue creada para conectarse mediante cable coaxial pero en la actualidad puede usarse otros tipos de cable como el UTP.

Si se utiliza cable coaxial grueso, se puede tener hasta cinco tramos de cable (unidos con repetidores) y las estaciones se conectan al cable por medio de tranceptores (la distancia máxima entre la estación y el tranceptor es de 15 metros). Se pueden conectar estaciones en tres tramos únicamente, con un máximo de 100 estaciones en cada tramo.

La velocidad que alcanza este tipo de red es de 10 Mbps [12] a una distancia máxima de 2 Km.

La topología utilizada es de BUS, con un protocolo de contienda o acceso al medio CSMA/CD (Acceso múltiple por detección de portadora con detección de colisiones).

Token Ring.

Esta arquitectura fue diseñada por IBM a finales de 1985. Este tipo de red emplea una topología de anillo y como protocolo de acceso al medio usa un protocolo de paso de testigo y se puede utilizar, cable coaxial, par trenzado o fibra óptica.

La velocidad que alcanzan este tipo de redes es de 4 Mbps, pudiéndose conectar a una distancia máxima de 350 metros en cada Unidad de Acceso Multiestación (MAU) si se utiliza un cable coaxial. (si se utiliza fibra óptica puede llegar a una velocidad de 16 Mbps) No obstante se pueden conectar 12 unidades MAU, aumentando considerablemente el número de estaciones. [13]

Arcnet

Datapoint fue quien desarrollo este sistema, que comenzó como un sistema distribuido, aunque comercialmente fue distribuido por Standard Microsystems.

Es una mezcla de redes, en la que se une las topologías de estrella y bus, además del protocolo de acceso al medio de paso de testigo.

Es considerablemente más lenta que las otras dos, ya que alcanza una velocidad de 2.5 Mbps y todas las estaciones están conectados a un HUB. La distancia máxima no puede sobrepasar los 660 metros.

Se pueden conectar HUBs entre si por lo que el número máximo de estaciones es de 255.

Otros Dispositivos.

Para conectarnos con el exterior o simplemente extender nuestra señal, es decir que queramos transmitir datos con alguna otra red, o alguna estación distante contamos con otros dispositivos, entre los que se encuentran:

[12] Mbps. Mega Bits Por Segundo

- Repetidores.
- Bridges. (puentes)
- Routers. (encaminadores o enrutadores)
- Getaways. (Pasarelas)

Repetidores. Son los encargados de regenerar la señal entre dos segmentos de una red homogénea que se interconectan, ampliando su cobertura. Opera en el nivel físico del modelo de referencia OSI.

Su forma de actuar es muy sencilla, simplemente recoge la señal de que circula por el medio físico y lo reenvía por la misma red o por otra distinta sin afectarla o interpretarla.

Bridges. Simplemente nos sirve para conectar dos redes entre si, es un sistema formado por hardware y software. Puede ser colocado en algún servidor como el de archivos o de comunicación, sin embargo es necesario que estas redes utilicen el mismo protocolo para poder comunicarse. A diferencia de un repetidor, el puente actúa sobre los paquetes de datos o tramas que se transfieren en los niveles de enlace de datos. Particularmente sobre el nivel de control de acceso al medio.

Sus funciones básicas son las de autoaprendisaje, filtrado y reenvió. Es decir, si necesita reenviar un paquete de datos a una dirección de red que no está incluida en su tabla de destinos, examina los campos de dirección del paquete (filtrado) y las dirige a la dirección que ha localizado (reenvió). A continuación, la añade a su tabla de destinos (autoaprendizaje).

Router. Un router no sólo incorpora la función de filtrado característica de los bridges, además, determina la ruta hacia su destino. A principio podríamos creer que un router y un bridge son lo mismo pero existen principalmente dos aspectos que diferencian a los routers de los bridges.

- El Router actúa sobre los paquetes tranferidos entre los niveles de red de la estaciones, a diferencia de los Bridges que lo hacen sobre el nivel de enlace de datos.
- Ambos equipos son, teóricamente, transparentes en las estaciones finales que comunican. Sin embargo, normalmente las estaciones tienen definido el router al que deben dirigirse.

[13] Fuente: http://www.3com.com/

Su funcionamiento es basado en un esquema jerarquico, que nosotros conocemos como las tablas de rutas o de ruteo. Generalmente estas tablas distinguen la dirección del dispositivo dentro de la red y la dirección fuera de la red, por lo que incorporan protocolos de nivel de red. Como el SNMP[14] que describire en el capitulo 4.

Getaway. También como en los anteriores, es un sistema formado por hardware y software que nos ayuda a comunicarnos con un mainframes o minicomputadoras. Utiliza los protocolos de nivel de transporte, sesión, presentación y aplicación. Por lo general se encuentra en el servidor de comunicaciones. Es el encargado de la traducción entre las familias de protocolos, proporcionando una conectividad completa entre redes de distintas naturaleza.

He explicado los conceptos más utilizados cuando se habla de redes, esto para que el lector tenga los conocimientos necesarios al momento de que explique conceptos más detallados, y en si mi propuesta de segmentación y administración de la red LAN de la ENEP Aragón. Es decir el objetivo de este capitulo no es tener apuntes para una materia de redes, o dar una cátedra de conocimientos relacionados, debido a que considero que esos temas son demasiado extensos para cubrirse en un solo capitulo. Por lo que recomiendo al lector, si el considera necesario para si mismo revisar en la bibliografía del presente trabajo y en internet conceptos más detalladas sobre redes.

[14] SNMP, Simple Network Managment Protocol

CAPITULO 2.

Situación actual y análisis de la estructura de la red de la ENEP Aragón

2.1 Análisis.

En está parte del proyecto describiré en forma detallada la situación actual del cableado, ubicación y tipo de los contentradores, topología, protocolos utilizados, aplicaciones de mayor trafico, direcciones IP. Es decir analizaremos con detenimiento la Red Local de la ENEP Aragón, para encontrar fallas y detalles que pudieran estar afectando el rendimiento de la Red.

Comenzaré con la descripción de un diagrama general, que describe la ubicación de los edificios conectados a la red LAN, y por que medio son conectados. Estos datos fueron recabados en Julio del 2000. Se debe tener presente la fecha de recopilación de los datos, debido a que constantemente las redes de este tipo sufren cambios ocasionados por los múltiples sistemas administrativos, es decir al no estar centralizada la administración de la Red LAN de la ENEP Aragón los cambios pueden ser imprevistos y desordenados, o simplemente no hay comunicación entre los administradores de la red LAN y estos cambios no son conocidos por las personas que deben saberlos.

En primera instancia se tiene el edificio de mantenimiento, que es el lugar en donde llega el enlace dedicado E1 vía microondas, es decir la señal de RedUNAM, que a su ves es reenviada a toda la ENEP por un router.

El medio de transmisión utilizado para la señal es el de fibra óptica, nos damos cuenta mediante el diagrama de la figura 5, (se encuentra en la página 26). por que parte de la escuela llega este medio de transmisión a cada edificio de la ENEP. Cabe mencionar que en cada edificio en donde llega la señal de RedUNAM tenemos un cableado que puede variar a la fibra óptica, por eso se describiré más a detalle cada edificio en donde llega la señal de RedUNAM, mencionando el concentrador o concentradores a donde llega la fibra óptica, la topología usada en ese edificio,

las aplicaciones más utilizadas en los servicios y la direcciones IP ocupadas en ese edificio o segmento.

Tenemos 9 edificios conectados a RedUNAM y divididos en tres segmentos de direcciones IP, como podemos observar en la tabla siguiente:

Edificio	Segmento de red:
A1 (Servicios Escolares)	132.248.44.0
A4 (Fundación UNAM)	132.248.173.0
A5 (CAE antes CIDIC)	132.248.173.0
A12 (Posgrado)	132.248.145.0
Biblioteca	132.248.44.0
Centro de Cómputo	132.248.145.0
Centro Tecnológico	132.248.173.0
Gobierno	132.248.44.0
Laboratorio L-3	132.248.173.0

Tabla 1. Segmentos de red por edificios en la ENEP Aragón.

EL diagrama de la figura 5 es claro al mostrar los segmentos de red mediante colores, además de indica que la fibra óptica forma una "estrella" con el edificio de mantenimiento, sin necesidad de regresar al router. Ocasionalmente podría pensarse que la fibra óptica es reenviada a otro edificio sin embargo esto no es cierto, ya que, la fibra óptica para optimizar conductos es enviada a distintos lugares por el mismo conducto físico.

Durante el levantamiento de información pude constatar que ésta es la distribución que debería estar en la ENEP Aragón, sin embargo, encontramos direcciones repetidas o en un lugar que no le correspondía, de acuerdo a la tabla 1 mostrada anteriormente. Por ejemplo: direcciones del segmento 132.248.44.0 en el edificio de posgrado. También en algunos casos los datos no fueron posible de levantar debido a que se encontraban en lugares fuera del alcance del personal de la propia ENEP Aragón o con etiquetas con datos inverosímiles debido al mismo estudio que se está realizando.

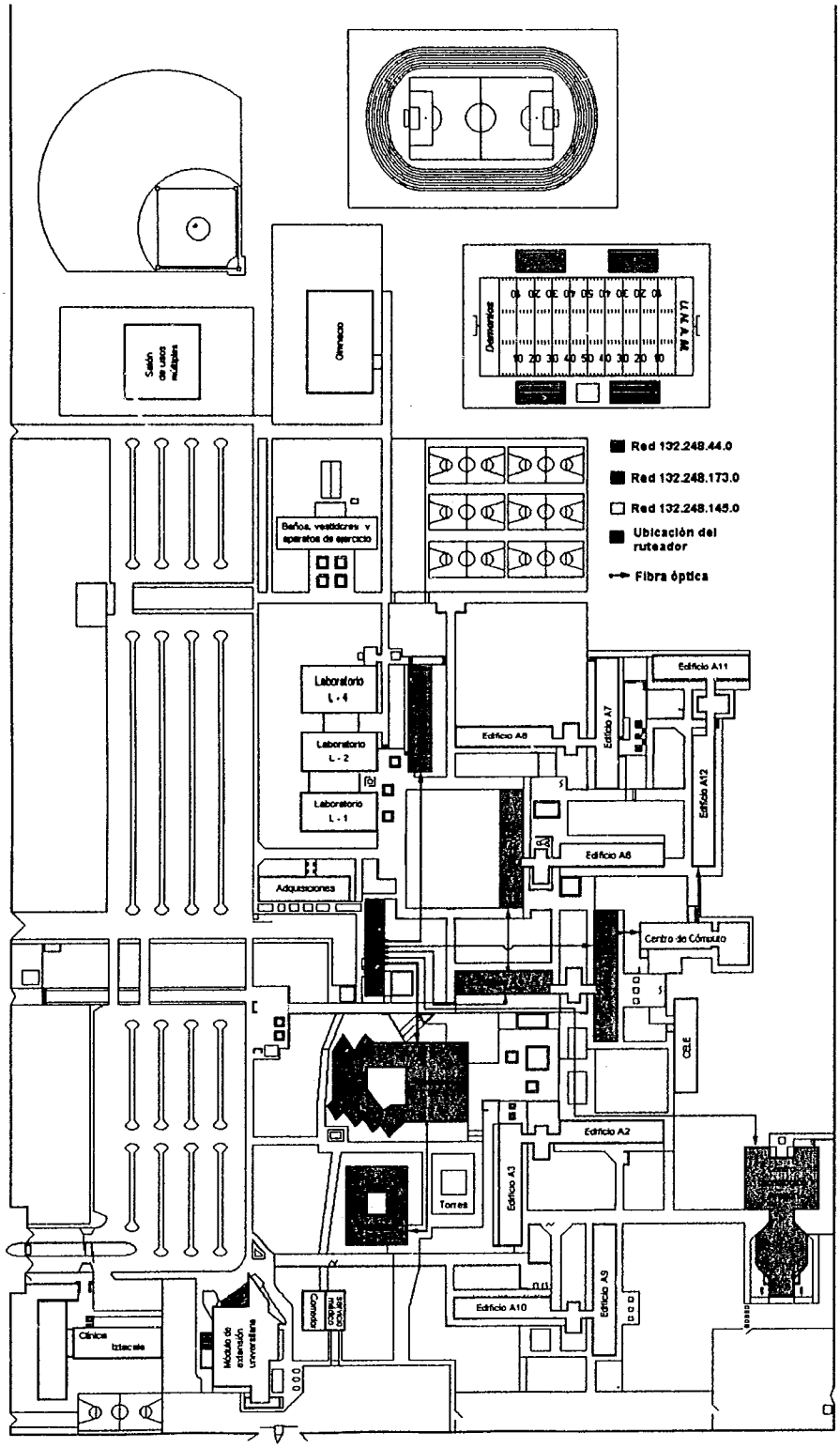


Figura 5. Mapa de Red de la ENEP Aragón

Edificio de mantenimiento

Este edificio es en donde se encuentra el ruteador que retransmite la señal de RedUNAM, primero recibe la señal, de una antena de microondas, la cual es enviada a un "Router CISCO 3000" por cable coaxial.

Este ruteador a su vez envía la señal por un transiver (de 24 hilos de fibra óptica) a los edificios en donde se conecta RedUNAM, esté transiver cuenta con 12 pares de hilos de fibra óptica de los cuales 11 pares están ocupados y el último par esta dañado. Describiré más adelante la conexión y servicios de cada unos de estos edificios.

A1 (Servicios Escolares)

A este edificio la señal de RedUNAM le llega a través de fibra óptica que sale del edificio de mantenimiento, en el edificio llega a un transiver el cual tan solo tiene como función recibir la fibra óptica y puentear la misma fibra óptica al Concentrador (HUB) de par trenzado.

Aquí se cuenta con un solo Concentrador "3com" modelo "SuperStack II PCHub 40" con 24 puertos, los cuales todos están ocupados por que tiene un cableado estructurado UTP, esto significa que las rosetas pueden o no tener una máquina conectada pero si tiene señal para conectarse a RedUNAM, como se verá más adelante en los servicios y aplicaciones de este edificio.

Se puede observar que físicamente llegan 8 hilos de fibra óptica de los cuales un par (Tx / Rx) es para Servicios Escolares otro par para Centro de Cómputo y un tercer par el cual tiene una etiqueta de "Informática", sin embargo el departamento de informática de la ENEP Aragón recibe la señal de RedUNAM por otro par de hilos debido a que esta unidad administrativa se cambio al edificio de gobierno. Asi lo mostraré más adelante en el estudio del edificio de gobierno. Quedando de está manera 2 pares de F.O[15]. Libres

En este edificio contamos con tarjetas para la red de tipo Ethernet, con una topología física de estrella pero lógica de bus, por el tipo de concentrador utilizado. Este edificio cuenta con 12 direcciones IP por el momento, del segmento 132.248.44.0. como lo muestra la siguiente tabla.

[15] F.O. Fiber Optic, Fibra Optica

Nombre	Dir. IP	Tipo de Tarjeta, Configuración y Ubicación		Fecha [16]
SEVESC1	.206	3c503 0x62 3 0x300		VI-97
SEVESC2	.207	3c509 0x62 10 0x300	Longshine LCS-8634 10 0x300	VI-97
SEVESC3	.208		Sun Sparc Station 4	VI-97
SEVESC4	.209	3c509 0x62 10 0x300	Escolares	VI-97
SEVESC5	.210	3c503 0x62 3 0x300	Egresados	VI-97
SEVESC6	.211	3c509 0x62 10 0x300	Jefe de servicios Esc.	XI-98
SEVESC7	.212	3c509 0x62 10 0x300 con UTP y coaxial		
Disponible	.213			
Disponible	.214			
Disponible	.215			
Disponible	.216			
Disponible	.217			

Tabla 2. Servicios ocupados en el Edificio de Servicios Escolares

Descripción de la Tabla.

- Nombre: Nombre asignado internamente al equipo (host) que cuenta don la dirección IP.
- Dir. IP: Dirección IP utilizada por el equipo, solo se muestra el ultimo bloque del segmento.
- Tipo de tarjeta. Controladores utilizados por la tarjeta de red en ese equipo.
- Ubicación: Lugar físico en donde se encuentra el equipo.
- Fecha: Mes en el que fue agregada la dirección IP al segmento de red.

Aquí destaco con color rojo una estación de trabajo, la cual pertenece a DGAE[17], que es un equipo con más carga de trabajo, ya que es utilizado para la base de datos de alumnos de la ENEP Aragón. la cual es transmitida vía TCP/IP a C.U. por lo que la comunicación con RedUNAM debe estar siempre en optimas condiciones.

A4 (Fundación UNAM).

Este edificio aunque cuenta con responsable propio depende directamente de la administración del C.C.C.A. La fibra óptica le llega directamente del edificio de mantenimiento y por

[16] Datos obtenidos del personal de que cada edificio.

el mismo conducto físico se envía la señal de RedUNAM al edificio A 5. En la mayoría de los edificios se recibe la fibra óptica a través de un convertidor que la direcciona a los concentradores, este edificio no es la excepción, aquí se cuenta con 2 concentradores apilados 3com SuperStack II PC Hub 40 de 24 puertos cada uno.

Los servicios prestados en este salón son solo de préstamo de PC's cuentan con algunas aplicaciones como "Office de Microsoft", lenguajes de programación, Software de conexión a RedUNAM, entre otras.

Las direcciones IP con las que cuenta este salón son de la red 132.248.173.0 entre el rango de direcciones de la .98 a la .145. no cuenta con servidores o estaciones de trabajo de punto critico.

A5 (CAE antes CIDIC).

Este edificio cuenta con un salón (A504) acondicionado para dar cursos y realizar desarrollos de software, antes se le llamaba CIDIC ahora se le nombra CAE. Como en los casos anteriores la señal es enviada por medio de fibra óptica y recibida por un transiver "ISO LAN 16805".

Aquí encontré 3 concentradores ubicados en distintas secciones del salón sin embargo estos se encuentran en cascada, cada concetrador es de distinto tipo, por lo que realice la siguiente tabla descriptiva de las características necesarias para este proyecto de cada uno de los concentradores.

Nivel de Escalamiento	Modelo del concentrador	Puertos Utilizados
1	3com Superstack 2 hub 10 con 16 puertos	2
2	3com Superstack 2 hub 10 con 16 puertos	8
3	3com Superstack 2 hub 40 con 24 puertos	18

Tabla 3. Caracteristicas de cada concentrador ubicado en el CAE

En el transiver no existe ninguna señalización de donde proviene la fibra óptica por el análisis la señal llega directamente del router es decir del edificio de mantenimiento. Del transiver la señal pasa al primer nivel de escalamiento, y así sucesivamente. Esté segmento pertenece a la red 132.248.173.0, como se muestra en la siguiente tabla.

[17] Dirección General de Asuntos Estudiantiles

Nombre	Dir. IP	Tipo de Tarjeta y Configuración	Fecha
ServerNT	.146		5-00
PC1	.147		5-00
PC2	.148		5-00
PC3	.149		5-00
	.150	Dirección IP Ocupada en otro segmento, tomada sin autorización	
PC5	.151		5-00
PC6	.152		5-00
PC7	.153		5-00
PC8	.154		5-00
PC9	.155		5-00
PC10	.156		5-00
PC11	.157		5-00
PC12	.158		5-00
PC13	.159		5-00
PC14	.160		5-00
PC15	.161		5-00
PC16	.162		5-00
PC17	.163		5-00
PC18	.164		5-00
	.165		
	.166		
	.167		
	.168		
	.169		
	.170		
	.171		
	.172		
	.173		
	.174		
	.175		
	.176		

	.177		
	.178		
	.179		
PC19	.180		5-00
	.181		

Tabla 4. Servicios ocupados en CAE.

La tabla hace que notar en esta red se tiene pocas direcciones IP ocupadas y sin embargo tiene el nivel máximo de escalamiento aceptable. También marco los puntos críticos para este segmento como lo es un servidor primario de dominio de NT y una dirección IP con problemas de duplicidad. La administración de este segmento se hace por alumnos que no llevan un control detallado de la red, solo conocen que los servicios tienen tarjetas de red Ethernet por consiguiente su topología es Ethernet y lógicamente es un bus.

A12 (Posgrado).

Este edificio anteriormente era uno de los más problemáticos debido a que utilizaba cable coaxial como medio de comunicación, además este cable coaxial no tenia las especificaciones técnicas necesarias para una red LAN, actualmente esta red ha sido reestructurada por parte de miembros de la DTD, se ha instalado cable UTP.

El concetrador, transiver, fibra óptica y demás dispositivos se encuentran en una caja negra la cual no puede ser abierta ya que se encuentra cerrada y la llave la tienen la gente que fue a instalar los servicios (DTD). Aunque a través del cristal podemos observar que: existe un transiver el cual recibe la fibra óptica y ésta es enviada a un concentrador "3com" modelo "Superstack II PC Hub 40" con 24 puertos, todos los puertos de este concetrador se encuentran ocupados.

La siguiente tabla muestra los servicios ocupados por RedUNAM, además señalo el servidor de mayor caga de trabajo. Este edificio es perteneciente al segmento 132.248.145.0.

Nombre	Dir. IP	Tipo de Tarjeta y Configuración		Fecha
POST2	.206	3c509 0x62 10 0x300	(Jefatura de Posgrado)	VI-97
POST5	.207	3c509 0x62 10 0x300	(Coordinación de Investigación)	VI-97
POST1	.208	3c509 0x62 10 0x300	(Especialización en Puentes)	VI-97
	.209		(Economía Financiera)	VI-97
POST4	.210	3c509 0x62 10 0x300	(Posgrado Sección Escolar)	VI-97
	.211		(Sria. Aca. De Ciencias Políticas)	VI-97
	.212		(Sria. Tec. Aca. De Posgrado)	VI-97
	.213			
	.214			
	.215			
	.216			
POSGRA	.217	DAVICOM 9102	SERVIDOR NT	III-99

Tabla 5. Servicios utilizados en Posgrado.

Como en las tablas anteriores del mismo estilo, se destaca con un color diferente el servicio con mayor carga de trabajo, en este caso se cuenta con un servidor NT. El cual según la propia gente del edificio de posgrado y del departamento de informática es el servicio con mayor carga, debido a que se utiliza para compartir archivos.

Biblioteca.

La Biblioteca es uno de los últimos edificios a los cuales se le instaló cableado estructurado, el rack en donde se encuentra tanto la llegada de la fibra óptica como los concetradores está a mano izquierda de la entrada principal.

La biblioteca cuenta con 2 concentradores "3com" modelo "Superstack II PC Hub 40" con 24 puertos cada uno, estos concentradores están conectados en cascada, y van directo a un Path el cual tiene una función de solo puenteo entre los concetradores y las rosetas en donde se encuentra el cable UTP. Los 24 puertos del primer concentrador se encuentran ocupados

A estos concentradores les llega la fibra óptica directa del edificio de mantenimiento, en donde se puede observar 8 hilos de fibra óptica, de lo cuales un par (Tx / Rx) es para la biblioteca, otro continua y es enviado para el edificio de gobierno y el ultimo par queda libre. Estos datos son los encontrados en la caja de recepción de fibra óptica.

En la siguiente tabla muestro los direcciones IP ocupadas por la administración de la biblioteca y el departamento de Informática. Estos datos fueron proporcionados por el departamento de informática. Debemos recordar que este edificio es parte del segmento 132.248.44.0 como lo muestra el mapa de la figura 5. Se cuenta con 12 direcciones o servicios de red de los cuales 7 están ocupados.

Nombre	Dir. IP	Tipo de Tarjeta y Ubicación		Fecha
Oftec	.194	S/D [18]	Oficina técnica	VI-97
S/N [19]	.195	S/D	REVISAR	
S/N	.196	S/D	Credenciales	VI-97
S/N	.197	S/D	Adquisiciones	VI-97
S/N	.198	S/D	Préstamo Externo A	VI-97
S/N	.199	S/D	Préstamo Externo B	VI-97
S/N	.200	S/D	Oficina Técnica (circula)	VI-97
Disponible	.201			
Disponible	.202			
Disponible	.203			
Disponible	.204			
Disponible	.205			

Tabla 6. Direcciones IP utilizadas en la Biblioteca.

Centro de Cómputo.

El Centro de Cómputo de la ENEP Aragón es el edificio con mayor carga en nuestra red, por lo mismo es en donde se pueden encontrar mayor número de problemas. Además de contar con tecnología obsoleta que se utiliza en algunas secciones del edificio, la falta de recursos ha desarrollado el ingenio del personal para reutilizar equipo viejo, como tarjetas de red, cable coaxial y terminales para el funcionamiento del mismo. Es importante señalar que esta tecnología fue en su momento la más moderna, sin embargo no se ha podido actualizar.

Por el mismo conducto por donde llega la señal de Red UNAM al edificio de servicios escolares, llegan un par de hilos de fibra óptica a un COFOT que es el encargado de enviar la señal a un concetrador de cable coaxial, esta es una de las partes criticas del C.C.C.A debido a

[18] Sin Datos
[19] Sin Nombre

que existe una gran cantidad de equipos conectados con cable coaxial para tráfico de Novell y algunos servidores con TCP/IP, de aquí se toman 6 hilos de cable coaxial para distribuir la señal a distintos salones y uno para enviarlo a un concentrador que transforma el medio a Par Trenzado, en donde tenemos un alto nivel de apilamiento y cascadeo entre varios concetradores 3com. El siguiente figura muestra esta estructura.

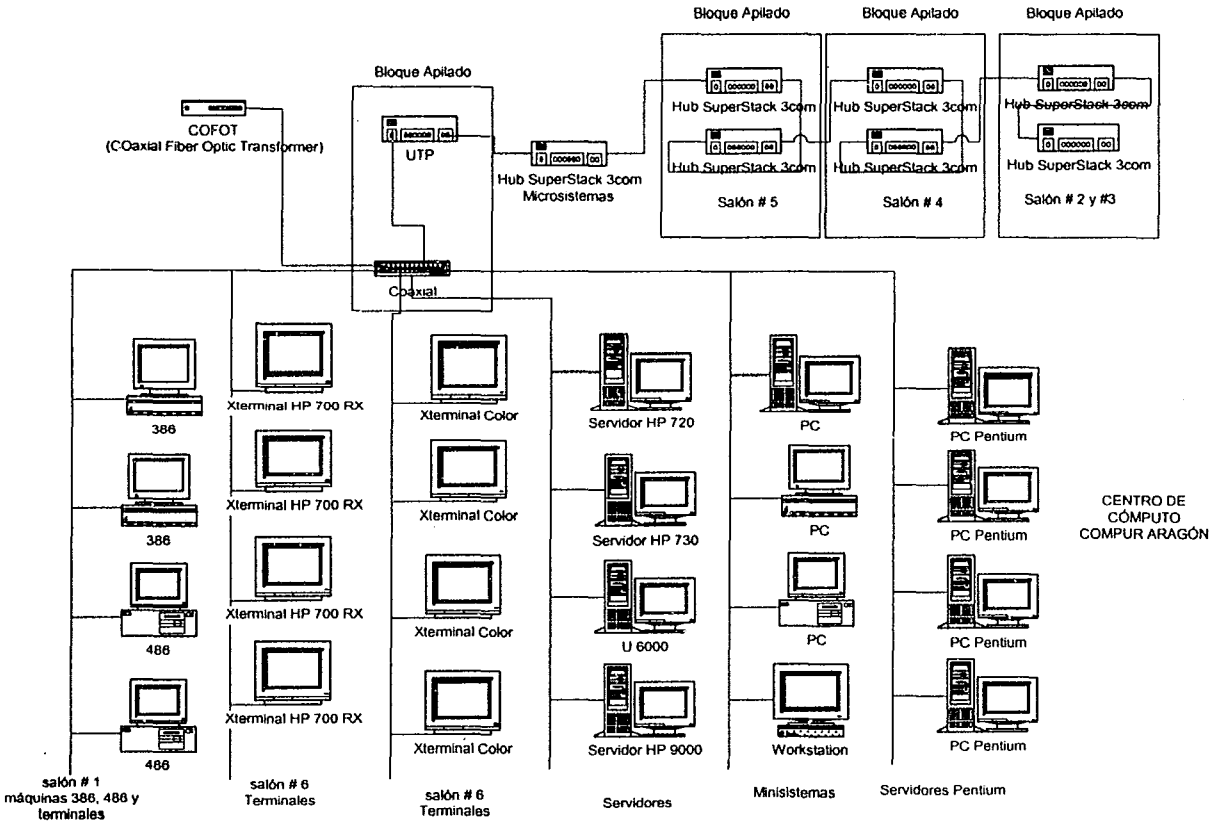


Figura 6. Diagrama de configuración del C.C.C.A.

En la figura 6 se puede observar la distribución física de los dispositivos más importantes en la red del C.C.C.A, este es uno de los edificios con mayor número de equipos, por lo que para una mejor comprensión de la topología se presenta un esquema de los equipos conectados, la distribución original solo varía en cantidad de equipos en cada sala. Como anteriormente mencione estos equipos datan de principios de los 90's, y en su momento era una moda el Cable Coaxial, por lo que esté equipo cuenta con dispositivos de red integrados de fabrica con dicha tecnología, lo que ocasiona que el remplazo de cable coaxial por par trenzado en estos equipos sea costoso. Un ejemplo de esto es el servidor de páginas web del C.C.C.A., por lo se esté problema se debe analizar por a parte, y cuyo estudio no esta en el alcance de este proyecto.

El edificio de C.C.C.A pertenece a la red 132.248.145.0 y sus rango es de la dirección 132.248.145.2 a la 132.248.145.205, dentro de este rango la información y ubicación de las direcciones varia, pero conservando un patrón ya que las direcciones de la .2 a la .50 son servidores de servicios de Internet, como correo electrónico, servidores web, ftp, gopher, y de trabajo bajo UNIX. Esta información es considerada como confidencial por parte de la administración de C.C.C.A. Los servidores con mayor caga de trabajo son dos el "hp-720" y el "indy" uno da al servicio de correo electrónico del Campus Aragón ya sea para estudiantes, profesores, autoridades administrativas y es el 132.248.145.2 mejor conocido como el servidor "hp-720" y el servidor de las páginas web del campus, el 132.248.145.5 también conocido como el "indy".

Centro Tecnológico.

El Centro Tecnológico tiene una de las infraestructuras de red mejor planeadas de la ENEP Aragón, esto debido a que es el edificio de más reciente construcción en la ENEP Aragón. Cuenta con cableado estructurado en todo el edificio. Tiene un panel de "ponchado" en la planta baja del edificio reduciendo así en gran medida el cascadeo en los hubs, y un hub 3com Superstack con 24 puertos uno en cada nivel, luego entonces tenemos 3 hubs en todo el edificio, un detalle que no afecta el rendimiento de la red pero si su administración es que en el segundo y tercer hub *(primer y segunda planta)* no se cuenta con un panel extra que ayude al puenteo hacia los hubs o concentradores, siendo directamente conectadas las rosetas a los hubs en estos niveles.

Del edifico de mantenimiento llegan 4 pares de fibra óptica al centro tecnológico dos de entrada y dos que se encuentran libres. Como vimos al principio el Centro Tecnológico pertenece a la red 132.248.173.0 y tiene disponibles para su disposición de la dirección .2 a la .73 los servicios más importantes de este edificio son:

Nombre	Dir. IP	Tipo de Tarjeta y Ubicación		Fecha
Tigrina	.2	3com	Doctor Daltabuit (oficina)	IX-00
Bengala	.3	HP	Secretaria	IX-00
Leon	.4	HP	Ambiental	IX-00
Tigre	.5	3com	Tigre	IX-00
Gato	.6			IX-00
Ocelote	.7	3com	Cabina	IX-00
Linze	.8	HP	Energía y ambiental	IX-00
Chita	.9			IX-00

Leopardo	.10			IX-00
Puma	.11	HP	Pedro	IX-00
Guepardo	.12	HP	Computación	IX-00
Montes	.13	HP	Doctor Daltabuit (clase)	IX-00
Pampas	.14	HP	Computación	IX-00
Siberiano	.15	SUN	Seguridad	IX-00
Nieves	.16	HP	Computación	IX-00
Pantera	.17	HP	Comunicaciones	IX-00
Marsay	.18	3com	Servidor	IX-00
Kadkod	.19	3com	Computación	IX-00
Cougar	.20	HP	Computación	IX-00
Jaguarundi	.22	HP	Computación	IX-00
Tigrillo	.23	HP	Licenciada	IX-00
Jaguar	.24	HP	Materiales	IX-00
Gatomontes	.25		Impresora	IX-00
Quemador	.28	3com	Computación	IX-00
Marcewin	.30	HP	Computación	IX-00
	.32	3com	Silvia	IX-00
Licjul	.50	3com	Digitalización	IX-00
Seguridad01	.65	3com	Seguridad	IX-00
Seguridad02	.66	3com	Seguridad	IX-00
Seguridad03	.67	SGI	Seguridad	IX-00

Tabla 7. Direcciones IP ocupadas y de mayor carga en el Centro Tecnológico.

Como en los casos anteriores, resalte los servicios con mayor carga de trabajo, por consiguiente mayor flujo de información a través de la red. Como ejemplo de los detalles que se presentan en las redes mal planeadas se encuentro un problema que se podría resolver con la segmentación de red de LAN de la ENEP Aragón. Es un error de "time Out" que ocasionalmente envía la impresora del Centro Tecnológico (Gatomontes) debido al tráfico de innecesario que circula por toda la red. Los paquetes tardan en llegar al la impresora debido al largo camino que recorren al no estar segmentada la red. El tiempo de espera se termina y envía el error. Ocasionando que no se pueda imprimir hasta que la carga de trabajo en la red sea menor.

Gobierno.

El edificio de Gobierno junto con el C.C.C.A son los edificios que cuentan con un mayor número de direcciones IP asignadas. A partir de la remodelación del edificio se instalo cableado estructurado en éste, dando lugar a una mejor administración ya que anteriormente su infraestructura era con cable coaxial y tarjetas de red en mal estado provocaban un desempeño nada optimo en una de las partes modulares de la administración de la ENEP Aragón, la Dirección.

La red en la que se encuentra el edificio es la 132.248.44.0. La tabla 8 muestra las direcciones IP además marco en diferente color los servicios críticos.

Nombre	Dir. IP	Tipo de Tarjeta y Configuración		Fecha
	.2			
	.3			
	.4			
	.5			
	.6			
GOB1	.7	NE2000 0x62 5 0x320	(Jefatura de Economía)	II-95
GOB2	.8	NE2000 0x62 5 0x320	(Jefatura de Periodismo)	II-95
GOB3	.9	NE2000 0x62 5 0x320	(Jefatura de Sociología)	II-95
GOB4	.10	NE2000 0x62 5 0x320	(Jefatura de Diseño Industrial)	II-95
GOB5	.11	NE2000 0x62 5 0x320	(Jefatura de Rel. Internacionales)	II-95
GOB6	.12	NE2000 0x62 5 0x320	(Jefatura de Planif. P/D Agropec.)	II-95
SECTEMEC	.13	3c503 0x62 3 0x300	(Sría. Ing. Mecánica Eléctrica)	II-95
GOB8	.14	3c509 0x62 10 0x300	(Jefatura en Ing. Mec. Eléctrica)	II-95
GOB9	.15	3c503 0x62 3 0x300	(Sría. Ing. en Computación)	II-95
GOB10	.16	NE2000 0x62 5 0x320	(Jefatura Ing. En Computación)	II-95
GOB11	.17	3c509 0x62 10 0x300	(Sría. Ing. Civil)	II-95
GOB12	.18	NE2000 0x62 5 0x320	(Jefatura Ing. Civil)	II-95
GOB13	.19	3c503 0x62 3 0x300	(Jefatura de Pedagogía)	II-95
GOB14	.20	NE2000 0x62 5 0x320	(Jefatura de Arquitectura)	II-95
DER3	.21	3c509 0x62 10 0x300	(Jefatura de Derecho)	II-95
GOB16	.22	3c509 0x62 10 0x300	(Div. Hum. y Ciencias Básicas)	II-95
GOB17	.23	3c509 0x62 10 0x300	(Sección Acad. Físico Mat.)	II-95
GOB18	.24	3c503 0x62 3 0x300	(División de Ciencias Sociales)	II-95
GOB19	.25	3c503 0x62 3 0x300	(Oficina del Director)	II-95
GOB20	.26	3c509 0x62 10 0x300	(Periodismo)	II-95
GOB21	.27	3c509 0x62 10 0x300	(Sría. de Rel. Internacionales)	III-95
GOB22	.28	3c509 0x62 10 0x300	(Sría. Pedagogía)	II-95
DER1	.29	3c509 0x62 10 0x300	(Secretaria de Derecho)	II-95
GOB24	.30	3c509 0x62 10 0x300	(Secretaria de la Dirección)	II-95
GOB25	.31	3c509 0x62 10 0x300	(Secretaría General)	II-95
GOB26	.32	NE2000 0x62 5 0x320	(Secretaría Administrativa)	II-95
GOB27	.33	3c509 0x62 10 0x300	(Secretaría Particular)	II-95

GOB28	.34	NE2000 0x62 5 0x320	(Departamento de Presupuestos)	II-95
GOB29	.35	3c509 0x62 10 0x300	(Sec. Acad. De Educ. y Semin.)	II-95
GOB30	.36	3c509 0x62 10 0x300	(Sec. Acad. De Ciencias Políticas)	III-97
GOB31	.37	3c509 0x62 10 0x300	(Sec. Acad. De Dis. Y Construc.)	IV-97
GOB32	.38	pkt9008 0x62 10 0x300	(Sria. Tec. De Arquitectura)	I-98
GOB33	.39		División de humanidades y Artes	I-98
STADCS	.40	3c509 0x62 10 0x300	(Secretaria técnica administrativa de la división de ciencias sociales)	VI-98
	.41	3c509 0x62 10 0x300	(Secretaria técnica de economía)	VIII-98
SERSOC1	.42	3c509 0x62 10 0x300	(servicio social)	VIII-98
ICOSEC2	.43	3com netbiu	(Secretaria Técnica de ICO)	XI-98
ACAD3	.44		(Unidad Académica)	XI-98
UAEST	.45	Compatible	Unidad de Asuntos Estudiantiles	III-99
	.46			
PER4	.47	3c900 TPO 10 PCI	(Departamento de Personal)	XI-98
PER5	.48	3c900 TPO 10 PCI	(Departamento de Personal)	XI-98
PER6	.49	3c900 TPO 10 PCI	(Departamento de Personal)	XI-98
PER7	.50	3c900 TPO 10 PCI	(Departamento de Personal)	XI-98
PER8	.51	3c900 TPO 10 PCI	(Departamento de Personal)	XI-98
PRES3	.52	3c509 0x62 10 0x300	(Departamento de Presupuestos)	III-95
PRES1	.53	3c509 0x62 10 0x300	(Departamento de Presupuestos)	III-95
PRES2	.54	3c509 0x62 10 0x300	(Departamento de Presupuestos)	III-95
PER1	.55	3c509 0x62 10 0x300	(Departamento de Personal)	IV-97
PER2	.56	3c509 0x62 10 0x300	(Departamento de Personal)	IV-97
DER2	.57	3c509 0x62 10 0x300	(Secretaria de Derecho)	VIII-98
PER3	.58		(Departamento de Personal)	X-98
	.59			
PLANE1	.60	3c509 0x62 10 0x300	(Planeación Académica)	II-95
PLANE2	.61	3c509 0x62 10 0x300	(Diagnóstico y Evaluación)	II-95
PLANE3	.62	3c509 0x62 10 0x300	(Planeación Académica)	II-95
INFOR1	.63	3c509 0x62 10 0x300	(Jefe Dep. De Informática)	II-95
PLANE4	.64	NE2000 0x62 10 0x300	(Apoyo a Planeación #1)	II-95
PLANE5	.65	NE2000 0x62 10 0x300	(Apoyo a Planeación #2)	II-95
INFOR2	.66	3c509 0x62 10 0x300	(Departamento de Informática #1)	II-95
INFOR3	.67	3c509 0x62 10 0x300	(Departamento de Informática #2)	II-95
INFOR4	.68	3c509 0x62 10 0x300	(Departamento de Informática #3)	II-95
INFOR5	.69	3c509 0x62 10 0x300	(Departamento de Informática #4)	II-95
INFOR6	.70	3c509 0x62 10 0x300	(Departamento de Informática #5)	II-95
INFOR7	.71	3c509 0x62 10 0x300	(Departamento de Informática #6)	II-95
UASA	.72		Unida de Apoyo y Soporte Académico	IX-98
PLANE20	.73		Unidad de Planeación	III-99
PLAN30	.74	NE2000	Unidad de Planeación	III-99
PLAN31	.75	NE2000	Unidad de Planeación	III-99
NUEVA	.76			
	.77			
	.78			

	.79			
ACAD1	.80	3c509 0x62 10 0x300	(Unidad Académica)	III-95
ACAD2	.81		(Unidad Académica)	VI-97
	.82		(Revisión de Estudios)	VI-97
	.83			
	.84			
	.85			
	.86			
	.87			
	.88			
	.89			
PINKY	.90	3c509 0x62 10 0x300	(Informática. Máquina Láser C)	XI-98
	.91			
	.92			
HURACAN	.93	Silicon Graphics	(Informática)	I-97
Temas20	.94	3c509 0x62 10 0x300	(Departamento de Informática #7)	I-97
INFOR8	.95	3c509 0x62 10 0x300	(FUTURA 04)	II-97
Servidor2	.96	Sun Classic		IV-96
INFOR9	.97	3c509 0x62 10 0x300	(Departamento de Informática #8	II-95
Enep	.98	HP-9000		II-95
Informática	.99	Sun Sparc Station 4		
	.100			
	.101			
	.102			
	.103			
	.104			
	.105			
	.106			
	.107			
	.108			
	.109			
	.110			
	.111			
POS1	.112		POSGRADO	III-00
POS2	.113		POSGRADO	III-00
POS3	.114		POSGRADO	III-00
POS4	.115		POSGRADO	III-00
POS5	.116		POSGRADO	III-00
POS6	.117		POSGRADO	III-00
POS7	.118		POSGRADO	III-00
POS8	.119		POSGRADO	III-00
	.120			
	.121			
	.122			

	123			
	.124			
	125			
	.126			
	127			
	.128			
	129			
	.130			
	131			
	.132			
	33			
	.134			
	135			
	.136			
	137			
	.138			
	139			
	.140			
	141			
	.142			
	143			
	.144			
	145			
	.146			
	147			
	.148			
	149			
BIBLIO1	.150		BIBLIO	III-00
BIBLIO2	151		BIBLIO	III-00
BIBLIO3	.152		BIBLIO	III-00
BIBLIO4	153		BIBLIO	III-00
BIBLIO5	.154		BIBLIO	III-00
	155			
	.156			
	157			
	.158			
	159			
	.160			
	161			
	.162			
	163			
	.164			
	165			
	.166			
	167			
	.168			
	169			

	170			
	.171			
	.172			
	.173			
	.174			
	.175			
	.176			
	.177			
	.178			
	.179			
BIBLIO6	.180		BIBLIO	III-00
	.181			
	.182			
	.183			
	.184			
	.185			
	.186			
	.187			
	.188			
	.189			
PATR1	.190	3c503 0x62 3 0x300		II-95
PATR2	.191	3c503 0x62 3 0x300		II-95
PATR3	.192	3c503 0x62 3 0x300		II-95
PATR4	.193	3c503 0x62 3 0x300		II-95

Tabla 8 Direcciones IP y de mayor carga en el Edificio de Gobierno.

Se observar en la tabla 8 que algunas de las direcciones fueron "prestadas" a la Biblioteca y al edifico de Posgrado, lo que ocasiona un grave problema de segmentación en la red. Debido a la distancia física que hay entre los edificios de Gobierno, Biblioteca y Posgrado. Además puede ocasionar problemas de comunicación en una futura segmentación.

Laboratorio L-3.

Solo el laboratorio L-3 es el único de los laboratorios que cuenta con el servicio de Red UNAM, las tareas de este laboratorio no están relacionadas directamente con servicios de TCP/IP, por lo que esté laboratorio cuenta con relativamente pocos servicios en comparación con otros edificios, solo son ocupados dichos servicios por profesores para la investigación y consulta de correo.

Como en los demás edificios la señal de Red UNAM llega por fibra óptica del edificio de mantenimiento por 1 par de hilos Tx y Rx para transmisión y recepción; son recibidos por un

transiver "1000A3 LIU" que a su vez envía la señal a un concentrador 3com "LinkBuilder" FMS II 3C16672.

El rango de direcciones IP que están asignadas para este edificio es del 132.248.173.74 al 134.248.173.97. Se cuenta con 24 servicios, y la primer dirección es un servidor SUN SparcStation 4 (132.248.173.74), como podemos ver es un pequeño equipo, pero con servicio de paginas WEB.

Como se puede constatar en la tabla 8 las fechas de recopilación no se encuentran en todos los casos, debido a la poca administración o casi nula, sin embargo estos datos fueron tomados en su mayoría en diciembre de 1999 y actualizados hasta julio del 2000.

2.2 Protocolos Usados en la ENEP Aragón.

En las relaciones internacionales los protocolos son reglas formales de carácter. Así los protocolos minimizan los problemas causados por las diferencias culturales cuando varias naciones trabajan juntas. De la misma manera funciona un protocolo en el ámbito computacional, es decir son las reglas de comunicación entre diferentes plataformas y sistemas operativos, de ésta manera plataformas UNIX se pueden comunicar con plataformas NT o cualquiera que estas sean, siempre y cuando utilicen el mismo protocolo de comunicación.

Actualmente en la ENEP Aragón se utilizan debido a las plataforma de trabajo, distintos protocolos, como lo son el TCP/IP, IPX, y NetBIOS, sin embargo mi propuesta se basa en el uso principalmente del protocolo TCP/IP, por lo que describiré a mayor detalle este protocolo.

2.2.1 El protocolo TCP/IP

El TCP/IP es un grupo de protocolos desarrollados para interconectar redes de computadoras. Estos protocolos tienen una configuración escalonada. Intentaremos explicarla con un ejemplo. Supongamos para manejar el tráfico del e-mail. El primer nivel es el que el protocolo necesita para enviar el mensaje, identifica al remitente, al receptor y al texto del mensaje. Sobre el segundo nivel está TCP, el protocolo que controla que los datos remitidos lleguen con eficacia al objetivo. Para este propósito el mensaje se divide en datagramas, y el TCP cuida para que los datagramas alcancen correctamente el objetivo. Sobre estos dos niveles todavía hay otro protocolo, el IP, que cuida el encaminamiento de los datos en el Internet. Por último, tenemos un cuarto nivel: la interfaz (Ethernet, acceso serial, etc.).

BREVE HISTORIA DE TCP/IP

El periodo comprendido entre los 50`s y 60`s no fue un buen periodo para la interconexión en redes. Casi todas las computadoras operaban de un modo central y autónomo, ellas no estaban diseñadas para interconectarse con otros sistemas, este periodo estuvo incorrectamente diseñado, ya que el hardware, sistemas operativos, formatos de archivos, programas de interface gráfica y otros componentes fueron todos diseñados para trabajar solo con un particular tipo de sistema de cómputo, excluyendo a todos los demás.

En los finales de los 60`s, el Departamento de Defensa de los Estados Unidos (*United States Department of Defense DOD)* empezó a interezarse en algunas investigaciones académicas relacionados con el "switcheo" de paquetes en una red de área extendida (*WAN*). La idea básica era conectar redes dispersas geográficamente, y enviar datos en forma de paquetes a través de la WAN.

El concepto de paquetes puede ser explicado como sigue: Imagine que se tiene una carta demasiado grande para enviar y es materialmente imposible que quepa en un sobre pequeño; y tienes específicamente que usar ese tamaño de sobres. Entonces divide la carta en pequeñas secciones, metiendo cada sección en un sobre individualmente, con la dirección del destinatario en cada sobre, y se numera secuencialmente a cada sobre para que el destinatario pueda reensamblar la carta completa. La carta de la que estamos hablando es análoga a los datos que un usuario ha creado con una aplicación y desea enviar a otro. Los sobres representan a los paquetes en una WAN la información es puesta electrónicamente dentro de paquetes, que están direccionados, secuenciados y enviados a través de la red.

La parte del *Switcheo* se refiere al envío de paquetes a un destino. Ya que cada paquete es direccionado individualmente, ellos pueden ser transmitidos por diferentes rutas físicas para llegar a su destino final. Este método flexible de transmisión es llamado como "switcheo de paquetes".

La verdadera razón por la que el DOD estaba interesada en la investigación, era por que ellos querían crear una WAN que pudiera portar, comandar, y controlar información en el caso de una guerra nuclear. Ya que una red de este tipo podría tener muchos sitios dispersos geográficamente y los datos serían enviados de muchas formas, aunque hubiera una falla en algún punto de la red. Este también sería el comienzo de Internet.

La investigación armamentisia de la DOD fue en una agencia llamada "The Advanced Research Projects Agency" (*ARPA*), ahora llamada "Defense Advanced Research Projects Agency" (*DARPA*). La misión de este grupo fue el comenzar una investigación básica que pudiera contribuir

a los esfuerzos de defensa. Esta era la agencia que fundó y manejo el proyecto para crear el *switcheo de paquetes WAN.* Los científicos y los ingenieros que fueron reclutados para este proyecto provenían de las mejores universidades y de las empresas privadas de Bolt, Beranek y Newman (BBN) en Cambridge, Massachusetts. El reto que ellos encararon estaba relacionado principalmente con dos ideas: interconectividad y interoperabilidad.

La interconectividad trataba con el transporte de información. Un Protocolo de Software era necesario, que pudiera empaquetar y encaminar información entre múltiples lugares. Fuera del concepto de *switcheo de paquetes WAN*, es así como el protocolo que eventualmente conoceríamos como IP, fue creado.

Con el problema de transmisión resuelto, el equipo movió sus investigaciones al siguiente objetivo la "Comunicación", es decir la interoperabilidad. Ya que de que servia poder enviar información fuerte y claro, si al recibir la información esta era incompresible por que ambos sistemas hablan diferentes lenguajes. Entonces la comunicación tiene que ser de aplicación a aplicación, ya que las aplicaciones estaban corriendo en diferentes plataformas de hardware con diferentes sistemas operativos, con diferentes tipos de archivos, diferentes tipos de terminales y mucho más. Un puente entre todas estas diferencias tenía que ser construido.

La solución fue desarrollar unas series de protocolos de aplicaciones estándar que permitieran la comunicación aplicación a aplicación y fueran independientes a las plataformas de hardware. Por eso podemos usar el mismo protocolo, de email en una mainframe o en una PC, siempre y cuando utilicen este protocolo. Este mismo principio se uso para crear protocolos estándar para transferencia de archivos, emulación de terminales, impresión, administradores de red y otras aplicaciones.

EL MODELO DOD.

El grupo de protocolos TCP/IP es esencialmente una integración de varias funciones de comunicación gobernadas por unas estrictas, y requeridas reglas de acuerdo a cómo ellos deben implementarse y representarse. El Modelo DOD, es similar en concepto al modelo OSI.

Tomando al modelo OSI (Open Systems Interconection) como referencia se puede afirmar que para cada capa o nivel que él define, existen uno o más protocolos interactuando. La comunicación entre protocolos es entre pares (peer-to-peer), es decir, un protocolo de algún nivel dialoga con el protocolo del mismo nivel en la computadora remota. Como lo ejemplifica la figura siguiente.

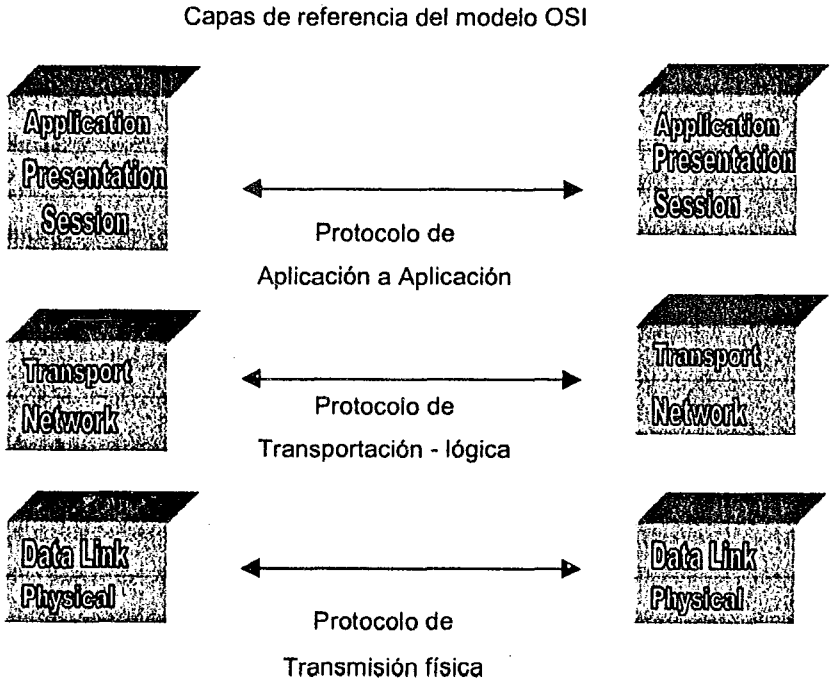


Figura. 7. Comunicación entre las capas del modelo OSI.

Las funciones propias de una red de computadoras pueden ser divididas en las siete capas propuestas por ISO para su modelo de sistemas abiertos (OSI). Sin embargo la implantación real de una arquitectura puede diferir de este modelo. Las arquitecturas basadas en TCP/IP utilizan el modelo de la DOD el cual propone cuatro capas en las que las funciones de las capas de Sesión y Presentación son responsabilidad de la capa de Aplicación y las capas de Liga de Datos (también conocida como de enlace) y Física son vistas como la capa de Interface a la Red. Por tal motivo para TCP/IP sólo existen las capas Interface de Red (Network Access), la de Intercomunicación en Red (Internet), la de Transporte (Host to Host) y la de Aplicación (Process/Aplication). Como puede verse en la figura 8, TCP/IP presupone independencia del medio físico de comunicación, sin embargo existen estándares bien definidos a los nivel de Liga de Datos y Físico que proveen mecanismos de acceso a los diferentes medios y que en el modelo TCP/IP deben considerarse la capa de Interface de Red; siendo los más usuales el proyecto IEEE802, Ethernet, Token Ring y FDDI.[20]

[20] Fuente: MCSE TCP/IP Exam Cram, Gari Novosel

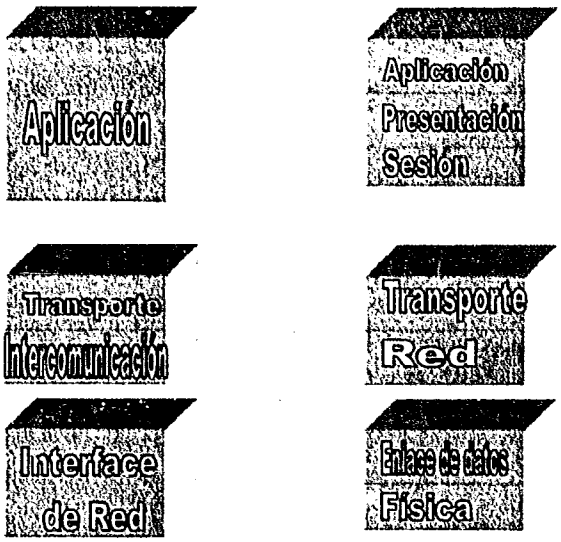


Fig.8
Comparación
Entre modelo DOD
Y Modelo OSI

Capa de aplicación *(Proccess/Aplication)* del modelo DOD.

Esta capa hace un llamado a los protocolos que utilizan servicios de la red, y que interactuan con algunos protocolos de la capa de transporte para enviar o recibir datos, ya sea como mensajes o simplemente como un flujo de bits. Dentro de estos protocolos podemos encontrar a, Telnet, FTP, SMTP, HTTP, SNMP, LDP, NFS, entre otros.

En esta capa podemos encontrar un vasto número de protocolos que se combinan para realizar las actividades de las capas de Sesión, Presentación y Aplicación del modelo OSI.

Capa de transporte *(Host to Host)* del modelo DOD.

Esta capa provee comunicación extremo a extremo desde un programa de aplicación a otro. Regula el flujo de información. Puede proveer un transporte confiable asegurándose que los datos lleguen sin errores y en la secuencia correcta. Coordina a múltiples aplicaciones que se encuentren interactuando con la red simultáneamente de tal manera que los datos que envíe una aplicación sean recibidos correctamente por la aplicación remota, esto lo hace añadiendo identificadores de cada una de las aplicaciones. Realiza además una verificación por suma, para asegurar que la información no sufrió alteraciones durante su transmisión. Dentro de esta capa podemos encontrar los siguiente protocolos TCP y UDP.

Capa de Intercomunicación en Red *(Internet)* del modelo DOD.

Controla la comunicación entre un equipo y otro, decide qué rutas deben seguir los paquetes de información para alcanzar su destino. Conforma los paquetes IP que será enviados por la capa inferior. Desencapsula los paquetes recibidos pasando a la capa superior la información dirigida a una aplicación. Esto lo hace direccionando cada paquete con lo que conocemos como dirección IP. Además de colocar un encabezado a cada paquete. Corresponde a la capa de Red del modelo OSI. Aquí es donde encontramos los protocolos de IP, como ICMP, BootP, ARP y RARP.

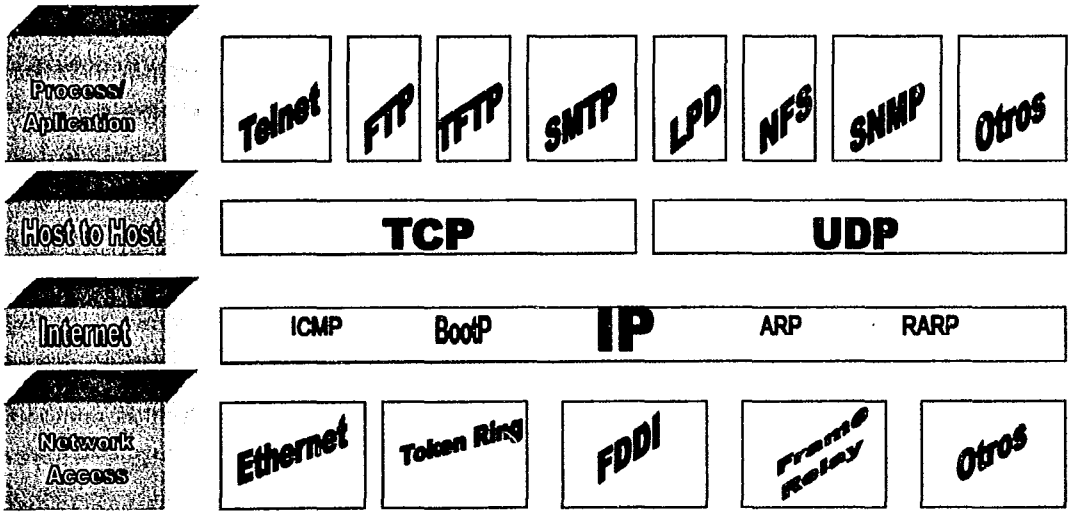
Capa de Interface de Red *(Network / Access)* del modelo DOD.

Esta capa monitorea el intercambio de datos entre el host y la red, es la equivalente a la capa de enlace de datos y física del modelo OSI.

Emite al medio físico los flujos de bits y recibe los que de él provienen. Consiste en los manejadores de los dispositivos que se conectan al medio de transmisión. Como Ethernet, Token Ring. FDDI, Frame Relay, y otros.

En la siguiente figura se observan los protocolos TCP/IP, dentro del modelo DOD.

Fig. 9. Modelo DOD y Protocolos TCP/IP



Modelo DOD **Protocolos TCP/IP**

Protocolo de Internet (IP)

El *Internet Protocol* es el corazón de TCP/IP y es el protocolo más importante de la capa de internet. IP provee el servicio de entrega de paquetes, todos los protocolos en las capas de encima y debajo del modelo jerárquico DOD utilizan IP para entregar los datos. En otras palabras IP se encarga de entregar los datos, sin embargo no es un protocolo orientado a la conexión es decir, no se preocupa por establecer la conexión con un diferente hosts, solo se encarga de enviar los datos.

Dentro de las funciones de IP tenemos:

- Definición del datagrama, que es la unidad básica de transmisión en el internet.
- Definición de un esquema de direccionamiento de internet.
- Mover los datos entre las capas de "Network Access" y de "Host to Host trasnport".
- Reenviar los datagramas a un hosts remoto.
- Revisar el performance de la fragmentación y reensamblaje de los datagramas.

Formato de los datagramas de IP.

Como he dicho anteriormente, un paquete es un bloque de datos que traen consigo la información necesaria para ser entregados, en una manera similar a como funciona el correo normal. Siendo así que el datagrama es el formato definido por el Internet Protocol para estos paquetes. El siguiente diagrama nos muestra este formato.

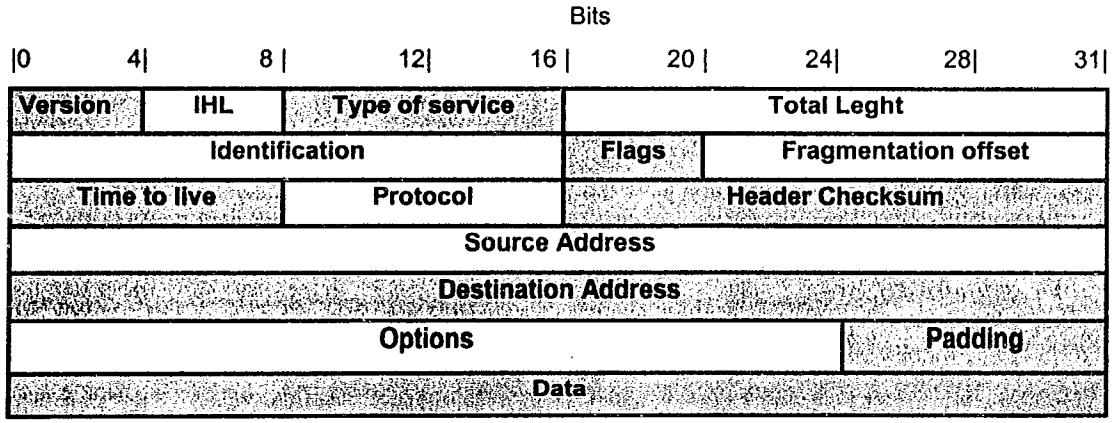


Figura 10. Datagrama IP

El datagrama consta de palabras que son cada uno de los renglones que tenemos en el diagrama, estas palabras tienen una extensión de 32 bits. Las primeras cinco o seis palabras de un datragrama forman el encabezado o header.

La sexta palabra es opcional por que el tamaño del encabezado es varible, por eso se incluye el IHL, "*Internet Header Legth*", este campo indica el tamaño del header en palabras. Este encabezado o header contiene toda la información necesaria para entregar la información.

La palabra más importante del "header" es la quinta; que contiene la dirección IP destino a la que se le entregaran los datos.

Protocolo de control de transferencia (Transfer Control Protocol. TCP)

El TCP (Transfer Control Protocol) divide los datos para ser enviados en datagramas, después tiene que volver a reensamblar los segmentos recibidos, y/o pedir el reenvío de los paquetes perdidos de los datos. El IP procede al encaminamiento (ruteo) de datagramas. Cada nivel del protocolo ignora completamente al otro, y de hecho cada protocolo agrega encabezados a los segmentos, de modo que sean únicos y sea difícil de que se pierdan en el camino.

En otras palabras TCP verifica que los datos han sido entregados correctamente, agregando un número consecutivo a su "header" para el reensamblado posterior de los datos, además de un campo de checksum que verifica que los datos que llegan no están corruptos. Como podemos se puede dar cuenta es el complemento perfecto para IP.

Formato del segmento de TCP

El segmento de TCP es muy similar al datagrama de IP, con la particularidad de que la información en los campos es la información necesaria para comprobar que los datos no están dañados, que puedan ser entregados y reensamblados correctamente. Lo mostramos a continuación.

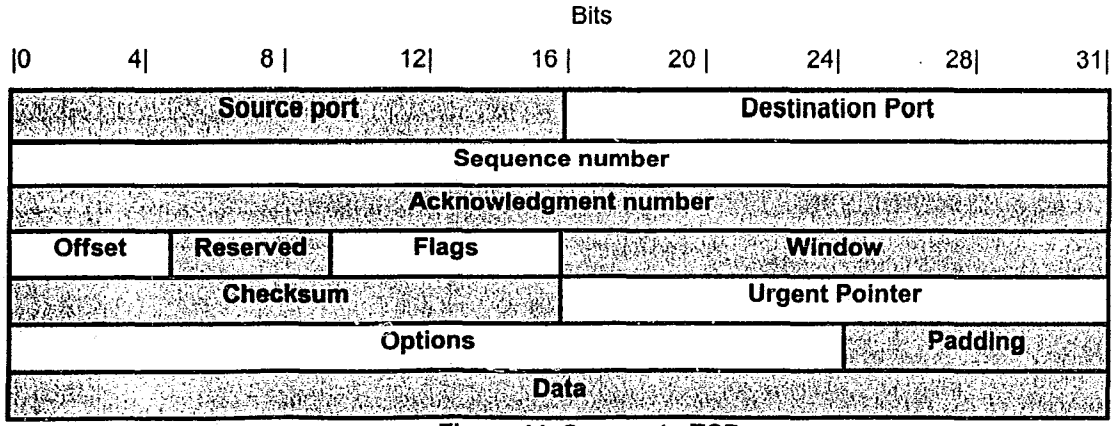


Figura 11. Segmento TCP

NETBIOS/NetBEUI

El NetBIOS (Networks Basic Input/Ouput System) es un protocolo de los niveles de red y de transporte del modelos OSI, desarrollado por IBM debido a la falta de normas estándar para los niveles superiores. IBM lo utiliza para proporcionar servicios de sesión, es decir que el NetBIOS mantiene la sesión enviando periódicamente un bloque de datos al nodo remoto para informarle de que se encuentra disponible y que puede recibir los datos, por lo que utiliza ciclos de memoria de manera continua aunque la aplicación del usuario no realice peticiones.

Estrictamente NetBIOS es una especificación de interface para accesar a los servicios de red. Resolviendo la recepción y envío de datos a través del nombre. Originalmente diseñado como un controlador para las PC Network LAN de IBM. Sin embargo las características de este protocolo han hecho de éste un estándar y diferentes programas usan el API[21] de NetBIOS para comunicarse sobre las redes IBM Token Ring, volviendo común el término de NetBIOS-compatible LAN, refiriendo al soporte de esta red con IBM Token Ring.

Esencialmente NetBIOS es un camino para los programas de aplicación para poder "hablar" a través de la red. NetBIOS estandariza la interface entre los programas de aplicación y las capacidades operativas de la red LAN, es decir una aplicación puede ser escrita para accesar solo los niveles más altos del modelo OSI haciéndola a ésta transportable entre diferentes ambientes de red. Este protocolo es soportado por las redes Ethernet, Token Ring y "PC Networks environment" de IBM.

El protocolo NetBEUI (NetBIOS Extender User Interface) es la extensión para NetBIOS uitilizada por LAN Manager, Microsoft Windows para trabajo en grupo, Windows 95, 98, NT y 2000.

NetBEUI también fue diseñado por IBM para su OS/2 LAN Server y e OS/2 Warp server, después éste fue adoptado por Microsoft para sus productos de redes. Esta extensión tiene todas las implementaciones del NetBIOS más algunas funciones como por ejemplo se le agregó el protocolo LLC2. Este protocolo corre bajo el estándar 802.2 de IEEEen el capítulo siguiente se explicará con un poco más detalle los RFC's [22] y estándares de IEEE[23]. El direccionamiento de paquetes de NetBEUI no permite el reenvío en las redes pero NetBIOS es adaptable a los protocolos que permiten el reenvío de paquetes como IPX y TCP/IP.

[21] Application Program Interface. Aplicamos el termino API, para los programas que sirven de front end y comunicación con otros sistemas diferentes para los que fueron diseñados.
[22] RFC = Request For Comments
[23] IEEE=Institute of Electrical Eloctronic Enginners

NetBEUI es muy rápido para las comunicaciones en una LAN, pero no tiene ruteabilidad para la comunicaciones en una WAN. Es por esto que nuestra propuesta se basa en el protocolo de TCP/IP. Aunque la importancia de este protocolo no se puede menospreciar si se necesita trabajar con redes de recursos compartidos de Microsoft.

IPX/SPX

Otro de los protocolos usados en nuestra escuela es el IPX/SPX, pertenecientes a las capas de red y transporte del modelo OSI. Estos protocolos fueron Desarrollados por Novell a principios de los años ochenta inspirándose en los protocolos del Sistema de Red de Xerox (XNS).

Sirven de interfaz entre el sistema operativo de red NetWare y las distintas arquitecturas de red (Ethernet, Arcnet, Token Ring).

Consiste en una variedad de protocolos iguales tales como:

- IPX (Internal Packet Exchange).
- SPX (Sequential Packet Exchange).
- NCP (Network Core Protocol).
- SAP (Service Advertising Protocol).
- RIP (Router Information Protocol).

Novell ha implementado también un emulador de NetBIOS para que las aplicaciones que utilicen NetBIOS puedan usar IPX como protocolo de red. Además, se utilizan los protocolos de Echo y Error para mantenimiento interno.

El nivel ODI (Open Data-link Interface) de Novell proporciona una función parecida a la del nivel de enlace de datos de OSI.

IPX: Este protocolo divide los datos en datagramas, de esta manera se mejora el rendimiento de la transmisión pero no pierde fiabilidad por dos razones:

- Cada bloque de datos IPX contiene una suma de comprobación CRC que garantiza un 99% de precisión.
- En caso de no haber contestación en un intervalo determinado de tiempo, IPX reenvía el paquete de forma automática.

SPX: el protocolo de transporte SPX es una extensión del protocolo de red IPX de superior nivel orientado a la conexión.

SPX utiliza IPX para enviar y recibir paquetes, pero añade una interfaz para establecer una sesión entre la estación emisora y la receptora, y de esta manera, se obtiene una confirmación explícita de la recepción del paquete. Además, proporciona un mecanismo de secuenciación de los paquetes. Como IPX envía los paquetes por el mejor camino disponible, es posible que éstos lleguen a la estación receptora en un orden distinto al que fueron enviados, lo que provoca que lleguen fuera de secuencia. Así, SPX de la estación receptora puede organizar los paquetes en un orden adecuado o reclamar únicamente los paquetes perdidos. Como podemos darnos cuenta funciona de una manera muy similar a la de TCP/IP.

NCP: Es un conjunto de mensajes bien definidos que controlan el funcionamiento del servidor y son la clave del acceso a los servidores NetWare.

Define el procedimiento que sigue Netware para aceptar y responder a las solicitudes de las estaciones. Existen protocolos de servicio NCP para cada servicio que una estación pueda solicitar a un servidor y, sin ellos, la estación no podría sacar ningún servicio del servidor.

Los NCP se pasan al servidor mediante paquetes IPX marcados de forma especial. No obstante, se pueden transmitir con cualquier otro protocolo de datagramas (como, por ejemplo, UDP de las redes basadas en TCP/IP.).

RIP: es un protocolo de información de encaminamiento que incorpora NetWare y que se encarga de llevar los paquetes a su destino entre dos redes.

Cada servidor realiza un seguimiento de los otros servidores a intervalos regulares y conserva si posición y distancia en una tabla de información sobre encaminamiento.

Si un servidor detecta una inconsistencia, un router existente lo notifica a los demás para que actualicen sus tablas. Si un router falla los demás lo cubren y buscan rutas alternativas que no toman en cuenta al router defectuoso.

SAP: Es una mecanismo mediante el cual NetWare distribuye información de los servidores disponibles por toda la red.

Necesita un servidor que anuncie tres unidades de información a la red cada minuto: el nombre del servidor, el tipo de servidor y su dirección de red.

El resto de los servidores descubre que se está desactivando, se lo indica a SAP y éste lo transmite a los demás servidores que lo guardan en su tabla correspondiente.

Si un servidor deja de transmitir sin previo aviso, SAP supone que no ésta disponible y lo transmite a toda la red para que actualicen su tabla.

De esta manera he terminado de hacer una análisis de los equipos concentrados en la Red LAN de la ENEP Aragón. Además de mostrar las características más importantes de los protocolos utilizados en la Red de la ENEP.

Esté estudio puede servirnos para identificar los principales problemas que tiene específicamente cada área y nos ayudará para la comprensión de la presentación la propuesta a la que hace referencia este trabajo. Como lo puede ser el nivel de cascadeo, el uso y las aplicaciones que tiene cada servicio de red, la falta de orden en la administración debido a que existen muchos encargados de red.

Las direcciones IP mostradas pueden ser un buen comienzo para la generación de un departamento que centralice la información y configuración de la Red LAN de la ENEP, ésta propuesta de administración la describo a mayor detalle en el cuarto capítulo de mi proyecto.

CAPITULO 3.

Propuesta de segmentación y reedireccionamiento para la red LAN de la ENEP Aragón.

3.1 Esquema actual de dispositivos de red.

En el capítulo anterior describí la manera en que cada edificio recibía la señal de Red UNAM, además del hardware utilizado en cada uno de los edificios.

En este capítulo propondré una nueva arquitectura para la Red LAN de la ENEP Aragón, sin embargo se necesita una visión más detallada a lo que me refiero con arquitectura, principalmente me refiero a las capas de Red y de Enlace de nuestra red. Para tener una mejor perspectiva de lo que se trata la propuesta la figura 12 muestra la situación actual desde el punto de vista necesario, mostrándonos solamente los dispositivos de red de capa 2 y 3 como concentradores (hubs), switches y routers, ésto para mostrarnos los niveles actuales de cascadeo y las conexiones que existen entre los edificios, estos son los datos que se descubrieron en el análisis mostrado en el capítulo anterior.

Después de este esquema explicaré las características de los dispositivos que usaré en la propuesta desde un punto de vista muy general hasta llegar al detalle específico de cada uno de ellos, finalizando con el mismo esquema de la Red LAN modificado con los dispositivos y tecnologías propuestas.

Estos diagramas de dispositivos se fueron actualizando hasta octubre del 2000, esta fecha es importante debido a que en ese preciso momento la situación de la Red LAN de la ENEP Aragón es la mostrada en el diagrama siguiente. Es lógico suponer que esta configuración puede cambiar rápidamente y probablemente en el momento de la publicación del presente trabajo ésta cambie, por lo tanto basaré mi propuesta en la configuración de este diagrama tomando en cuenta el mes de octubre del 2000 como punto de ubicación en el tiempo.

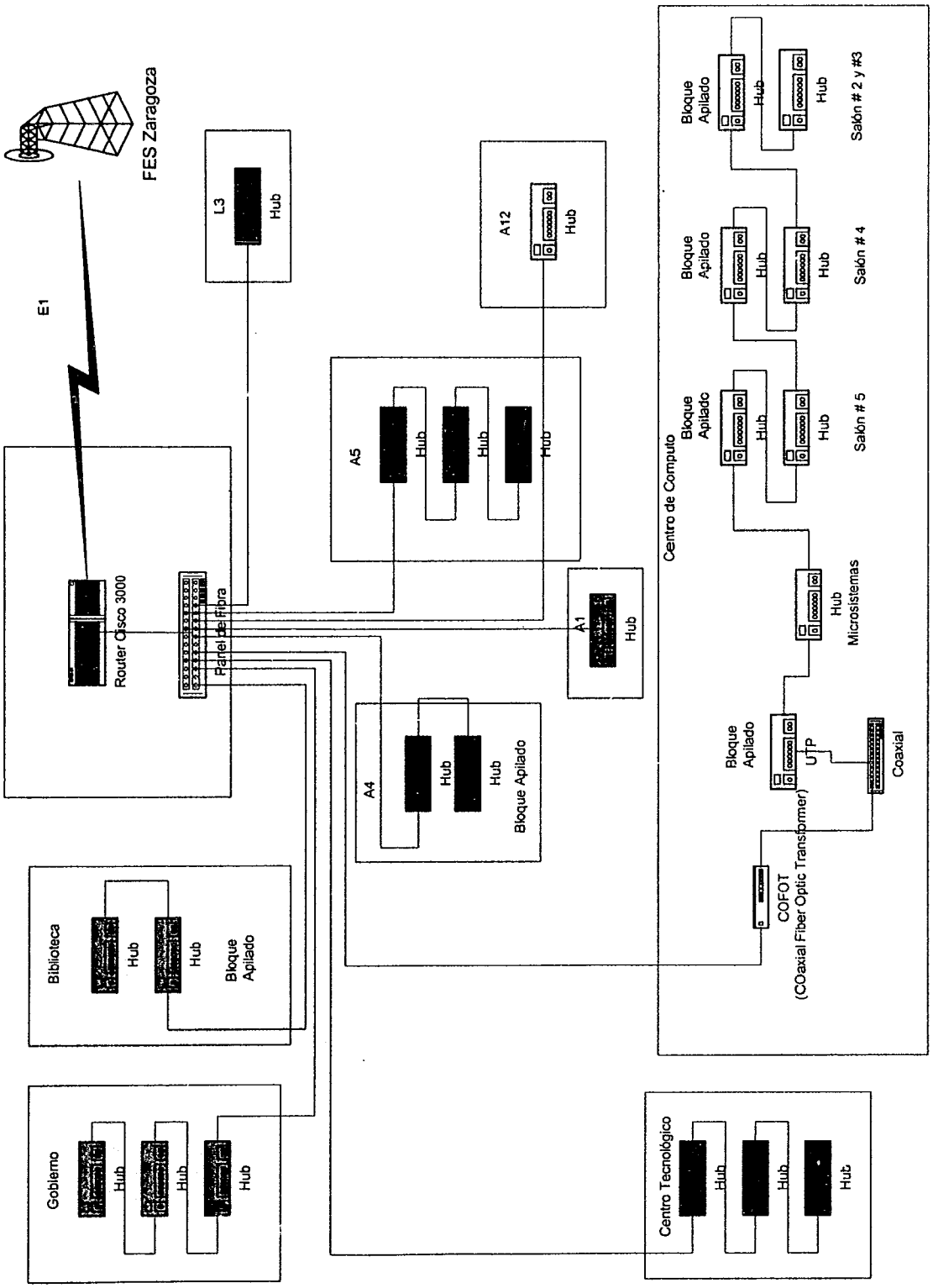


Figura 12. Situación Actual de dispositivos concentradores y router en la ENEP Aragón

3.2 Switches

El problema principal en la ENEP Aragón es el crecimiento desorganizado de la utilización de la misma, lo que ocasiona congestión de la RED LAN, por lo que el ancho de banda se ve reducido en general por:

- Las aplicaciones que continúan siendo transformadas de sistemas multiusuarios a redes LAN, y nuevas aplicaciones siempre se están desarrollando. Tal es el caso de la administración de horas en salones, mejor conocido como sistema CRONOS.
- Los servidores están centralizados en una computadora que sirve a sitios enteros o al campus en general. (servidores web, de correo).
- El bajo costo de la plataforma de servidores y computadoras de escritorio tiene el poder de procesamiento y capacidad para saturar el ancho de banda disponible. En otras palabras meter a la red a PC's innecesarias por tan solo meterlas.

Esto ocasiona principalmente problemas como:

- Cuellos de botella. (Mala Planeación)
- Colisiones. (Mayor uso más colisiones)
- IP's duplicadas. (Mala Administración)

Por eso el considerar las switched LAN o redes conmutadas por un switch son una muy buena opción para la red LAN de la ENEP Aragón, mi propuesta se basa en la implementación de algunos tipos de switches, describiré las características generales de estos.

Los switches LAN pueden permitir al proceso de microsegmentación ser extendidos a su última limitación para una sencilla estación terminal por segmento LAN, por ejemplo una conexión LAN dedicada o privada para cada usuario y servidor. Los switches LAN también pueden segmentar las redes lógicamente.

Una manera de pensar acerca de una switch LAN es como una especie de puente LAN o Brouter[24] de alta velocidad con una arquitectura donde muchos flujos de tráfico pueden ocurrir simultáneamente entre múltiples pares de puertos de entrada/salida. Los switches LAN también tienen las características de baja latencia o retardo y bajo costo por puerto. Los switches LAN son realmente una nueva generación de los puentes o brouters, la conmutación no está restringida a

[24] Dispositivo que reúne las mejores características de un router y de un bridge.

una tecnología LAN en particular. De esta manera, algún broadcasts[25] (para redes tipo Ethernet) o token passing (para redes token ring) la LAN puede ser conmutada, y por eso se puede esperar ver switches que soporten diferentes tipos de redes.

Los switches han surgido como una de las mejores soluciones para satisfacer las demandas de ancho de banda en las aplicaciones actuales (lentitud en la red, compartición de recursos) sin necesidad de buscar tecnologías complicadas y caras, proporcionando de esta forma la facilidad de que las computadoras donde residen las aplicaciones utilicen los medios de transmisión en forma simultanea y no serializada como en las redes compartidas.

Los switches se instalan en lugar de los concentradores convencionales formando una topología tipo estrella. Operan como si fueran Bridges o puentes de múltiples puertos pero de altas velocidades de conmutación. El colocar un conmutador Ethernet para interconectar segmentos con un total de 40 nodos por ejemplo, provoca un efecto tal, que el rendimiento medio en el switch permite que todos lo segmentos intercambien información entre sí, de manera que pareciera que se tiene un medio compartido cuyo ancho de banda es de 400 Mbps, cuatro veces más que 100 Base T. En redes conmutadas (switched LAN), cada nodo está conectado con un sólo enlace hacia el conmutador. Esto significa que en cierto momento, en ancho de banda en su totalidad está siendo utilizado por aquel nodo que transmite en ese momento; la velocidad de la línea no es proporcional al número de estaciones conectadas. En medios compartidos, todas las estaciones de trabajo deben competir entre sí para utilizar el ancho de banda. En soluciones de alta velocidad, los rendimientos se mejoran gracias a nuevos esquemas de codificación y señalización, que aprovechan mejor el ancho de banda disponible pero de todos modos ese ancho de banda deber ser dividido entre todos los nodos que quieren transmitir.

Tal es el caso de la Red LAN de la ENEP Aragón, ya que es una red de medios compartidos lo que significa que cada vez que tenemos un cascadeo o entre más nodos tengamos el ancho de banda se va dividiendo y el último nodo de la estructura tendrá solo un pequeño segmento del ancho de banda, lo que ocasiona la lentitud al momento de conectarnos a Internet y problemas para los usuarios en la Red LAN como lo son las colisiones.

Los switches soportan:

- Tecnologías de baja velocidad como ethernet y token ring.
- Conexiones entre estaciones de trabajo y servidores con interfaces ethernet, token ring y FDDI.

[25] Mensaje a todos los nodos de una red. En ocasiones es el encargado de transportar la información a través de la LAN.

- Tecnologías de alta velocidad como 100 base T (Fast Ethernet), FDDI (100 Mbps), ATM (25 Mbps) y 1000 Base R (Giga Bit E´net).
- Conexiones entre switches LAN y ATM.

La conmutación o switcheo en el acceso local reduce la carga en el backbone[26]. Los switches pueden sustituir a los hubs sin necesidad de cambiar adaptadores, cableado, tecnología de transmisión, etc.; inclusive los dispositivos de red pueden ser conectados directamente al switch. Características de uso:

- Los conmutadores o switches son mecanismos de intra-networking diseñados para incrementar el buen funcionamiento en la redes cliente/servidor.
- Habilitan accesos dedicados. Permiten el escalamiento en el ancho de banda de la red al incrementar la cantidad de puertos conmutados. (en caso de querer recibir un enlace extra podemos dedicar un enlace A para un segmento de la red y un enlace B para otro segmento de la red)
- Eliminan colisiones al 100% en el caso de redes totalmente conmutadas. (puerto de switch dedica por estación)
- Algunos switches facilitan la creación y administración de redes virtuales (VLAN's que es nuestra propuesta principal)

Como un conmutador telefónico, los switches soportan conversaciones simultaneas e incrementan la eficiencia en el uso del ancho de banda hasta en un 90%[27]. Las rutas de datos paralelas apoyan el incremento de salidas sobre la red; incrementando el ancho de banda, reduciendo o eliminando colisiones.

Un switch cuenta con:

- Microprocesador que le provee de inteligencia de alto poder para múltiples funciones.
- Content Addresable Memory (CAM) Memoria que almacena la tabla de direcciones MAC aprendidas.
- Application Specific Integrated Circuits (ASICs) Es un chip desarrollado para un proceso específico, diseñado para incorporar el estándar de CELLS. También se conoce como Gate Array, su única desventaja es que se desperdicia una parte considerable del chip.
- Tarjeta procesadora que consta de:

[26] Espina dorsal de la Red LAN, en donde se concentra el trafico de la red, el bus lineal en una red ethernet. En nuestro caso el backbone lógicamente es el panel de fibra óptica que se conecta al router.
[27] Fuente: http://www.cisco.com/

- Bus de Celdas. Se utiliza para proporcionar las capacidades de conmutación de celdas.
- Bus de datos o matriz de conmutación. Se usa para transferir los paquetes del puerto de entrada al puerto de salida.
- Bus de control. Realiza la interconexión, la secuencia y el control de los módulos conectados.
- Modulo de procesador espejo. (en algunos switches) Proporciona una función de redundancia.

Todos los switches están basados en implantaciones de software y hardware. La conmutación por hardware segmenta el bus dentro de otra matriz o bus conmutado. Los switches por hardware generalmente ofrecen rendimientos mejores, los switches por software usualmente ofrecen gran facilidad en la administración.

Conmutación basada en software. (software switching) la conmutación por software trabaja de la siguiente manera: un paquete entra al switch por software, en donde es sincronizado, convirtiendo la señal de serial a paralelo y examinando la información de direccionamiento. Una vez que esta en formato paralelo es escrito cíclicamente en una memoria rápida. El switch busca en su tabla de direcciones, para encontrar la dirección destino y establecer una conexión conmutada. Una vez que la conexión conmutada ha sido establecida, el paquete es leído de la memoria, reconvertido de formato paralelo a serial y transmitido vía conexión conmutada. Los switches por software están basados actualmente en una tecnología de ruteo que ha sido optimizada para conmutación de tramas o frame switching. Uno de los beneficios es que el switch por software se cuenta con una tecnología probada y funcional. Una de la mayores desventajas es que justamente como existen muchos ruteadores puede haber considerables configuraciones de trabajo.

La configuración de un switch por software es relativamente fácil de realizar, por que se fundamenta en el ruteo, y utiliza una arquitectura flexible, ya que puede facilitar la integración de conmutación y ruteo en redes que necesiten ambas funciones, lamentablemente la conmutación no es escalable y el rendimiento puede disminuir.

Conmutación basada en hardware (Hardware switching) Los switches basados en hardware en funcionamiento son parecidos a un puente o bridge, principalmente operan en la capa MAC, y existen dos tipos de switches basados en hardware, los matriciales o "crossbar" y los que utilizan una arquitectura de bus.

Switch basado en hardware con arquitectura de Matriz. Estos switches como su nombre lo indica basan su funcionamiento en una matriz punto a punto, en donde realizan conexiones entre direcciones MAC, es decir una trama entra por el puerto de entrada, viaja a través de la matriz hasta encontrar la intersección para la correcta dirección de salida. El switch puede soportar muchas conexiones puerto a puerto simultáneamente.

La dificultad con los switches de matriz, es su flexibilidad para adicionar puertos, puede ser complicado, las entradas deben ser igual a las salidas, lo cual hace difícil integrar un nuevo enlace para mayor ancho de banda. La administración también es una desventaja, ya que solo se puede monitorear una conexión a la vez.

Switch basado en hardware con arquitectura de Bus. Estos switches emplean un bus central sobre el cual todo el tráfico de el switch viaja. Pero usando un multiplexaje por división de tiempo, ya sea estadístico o estático, el switch da a cada puerto su propio turno para enviar un paquete en el bus, esto da como resultado un desempeño constante bajo diferentes cargas.

Expandir el switch es relativamente fácil por que las entradas no tienen que ser igual a las salidas. La arquitectura de bus es muy fácil de administrar, ya que tener un punto central sobre el cual todo el tráfico debe fluir permite monitorear todo el tráfico conmutado simultáneamente. Su desventaja es que tiende a ser caro.

En una arquitectura de switch:

- Los puertos físicos proporcionan la interfase física que conecta el equipo de los usuarios.
- Los puertos lógicos contienen las definiciones para varios servicios de transmisión.
- Los puertos virtuales toman los frames definidos y los presentan al puente virtual o router apropiado después de haber sido comparados contra la base de datos de reenvió.

En términos generales un switch permite:

- Crear grupos de trabajo que proporcionan mejor administración al poder realizar cambios por software y no por hardware.
- Proporcionar un ancho de banda dedicado para usuarios o grupos específicos, ya sea por Ethernet, token ring y/o en una transmisión hacia una red de alta velocidad, tal como FDDI, Fast Ethernet y/o ATM.
- Interconectar elementos de un sistema de computo distribuido a un sistema centralizado.
- Proporcionar conexiones de alta velocidad a servidores y backbones principales.

- Presentar alta disponibilidad y tolerancia a los errores.
- Flexibilidad de crecimiento a un alta ancho de banda.
- Modularidad.
- El Mezclado de diferentes tipos de LAN's.
- Sin limitaciones considerables en la velocidad del cable, debido al autosensing[28].
- Soporte de ruteo (capa 3).
- Administración de redes distribuidas.
- Cada Switch tiene la capacidad y la "inteligencia" de tomar decisiones para filtrar y enviar los paquetes de datos conforme la unidad de VLAN definida por el administrador de la red.

Tomando esto en cuenta describiré las características específicas de los modelos del router y switches utilizados en la propuesta. Por lo tanto los LAN Switches ofrecen importantes aumentos en el desempeño de nuestra RED Local, sin olvidar la facilidad para segmentar lógicamente la Red.

En esta propuesta se maneja un router Cisco 3640 por que cuenta con las características indispensables para la segmentación de nuestra red LAN con los switches.

Este router pertenece a una familia la serie 3600 de Cisco, esta familia combina acceso Dial Up, ruteo, servicios de LAN a LAN, integración de voz, video y datos en el mismo dispositivo. Todos lo routers de esta familia son productos modulares, cuentan con un software de configuración propietario de Cisco el IOS. Escogí el Cisco 3640, debido a que cuenta con 4 slots para módulos de red, de los cuales utilizaría 1 para el dispositivo que recibiría el enlace E1, y tres para cada uno de nuestros segmentos de red. La siguiente figura 13 muestra la parte de atrás este dispositivo en donde podemos apreciar dichos slots.[29]

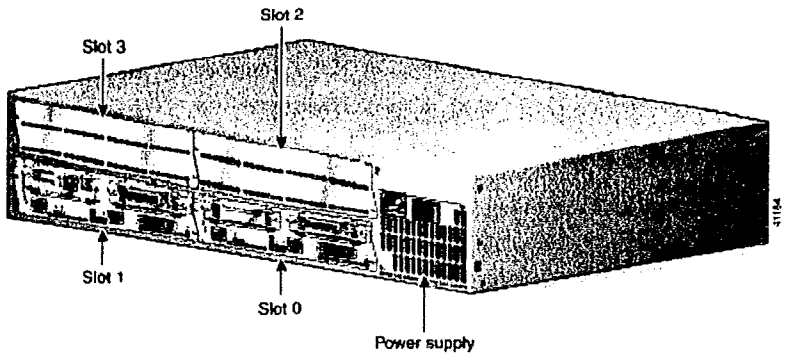


Figura 13. Router 3640 Cisco Corp. (Parte trazera)

[28] Autosensing.= La velocidad de transmisión del puerto del switch se ajusta automáticamente a la velocidad del medio y la tarjeta de red. (por ejemplo de 10 o 100 Mbps)
[29] Fuente: http://www.cisco.com/

Estos módulos que colocamos en los slots son intercambiables por lo que la escalabilidad es fácil en este dispositivo.

Existe una gran variedad de módulos que acepta esta familia de routers, la siguiente es una lista de los módulos que acepta, dando un abanico amplio de posibilidades de configuración.

- Módulos de red de voz analógicos y digitales. (T1)
- Interface "Single-Port High Speed Serial" (HSSI).
- Módulos de red ATM 25 Mbps.
- ATM OC3 155 Mbps.
- Módulos de 6,12,18,24 y 30 módems digitales.
- Módulos WAN. ("WAN Interface Card")
- Módulos de 8 y 16 módems analógicos.
- Módulos Canalizados de T1, ISDN PRI y E1 ISDN PRI.
- Módulos combinados de redes de Fast Ethernet y PRI.
- Módulos de 4 y 8 puertos de ISDN BRI.
- Módulos de 16 y 32 puertos de redes asíncronas.
- Módulos de 4 y 8 puertos de redes sincronas/asincronas.
- Módulos de 1 y 4 puertos de redes ethernet.
- Módulos de un puerto para redes Fast Ethernet. (100BaseT "TX" y Fibra "FX")
- Módulos de 4 puertos de red serial.
- Módulos de compresión de red.

Los switches seleccionados serían entonces 2 switches 3com SuperStack II 9300 con 12 puertos LX, la figura 14 muestra este tipo de switches, los puertos LX son los se utilizarán para generar 3 VLAN, las cuales serán explicadas más adelante. Y un switch 1100 para el Centro de Computo del Campus Aragón.

Los switches 9300 son una familia de switches de 12 puertos de fibra óptica dándole una velocidad de 100/1000 Mbps, teniendo así un performance de una Gigabit Ethernet (1000 Mbps), cuenta además con un software de administración llamado "Transcend Network Supervisor", que nos permite monitorear y administrar, sin algún cargo extra.[30]

Entre sus principales características tenemos:

- Todos sus puertos son "autosensing".

- Suporta mas de 16,000 direcciones MAC.
- Soporte para el estándar IEEE 802.3x para flujo de control en todos los puertos con Full-Duplex.
- Soporta RMON.
- Soporta IEEE 802.1Q VLAN's, es decir la principal característica para poder crear nuestras VLAN's.
- Administración vía browser.
- Total compatibilidad con equipo 3com.
- Soporta los estándares SNMP, RMON y MIB II.

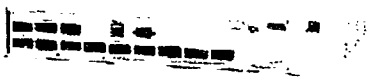


Figura 14. Switch SuperStack II 9300 3com

Debido a estas características este equipo es idóneo para la generación de las VLAN's de nuestra propuesta.

EL switch propuesto para el Centro de Cómputo es el 3com SuperStack II 1100 con 12 puertos. Debido a las funciones y modular que este presenta consideró que es el más aceptable para el problema encontrado en el Centro de Cómputo, que como hemos visto es el de mayor prioridad para resolver.

Con este switch podemos disminuir el cascadeo al máximo, además como ya mencioné cuenta con diferentes módulos que nos ahorrarían la necesidad de cambiar la infraestructura del C.C.C.A.. El modulo que menciono es el 3c1206-6 el cual no permite unir el segmento de cable coaxial existente a la segmentación de esta red.

Las características de este switch son muy similares al anterior.

- Totalmente escalable ya que reduce el costo al querer migrar nuestra red completamente a Giga Ethernet.
- Compatible con toda la línea 3com SuperStack II.
- Tiene la habilidad para integrar más de un switch dentro de nuestro esquema de red, y que se vea como uno solo. (Apilable)
- Software de administración incluido, mediante web.
- Soporta los mismos estándares de IEEE que el anterior switch.

[30] Fuente: http://www.3com.com/

- Gran performance para tráfico de tipo multimedia.
- Todos sus puertos son "autosensing 10/100 Mbps".
- Detección automática para comunicación Full/Half Duplex.
- Modularidad,
- Soporta RMON.

El modulo que propongo es el 3c1206-6 que es un transiver coaxial, 10base2 (BNC). Por donde llegará el segmento en donde se encuentra el servidor web del C.C.C.A. el cual tiene cable coaxial.

En resumen los dispositivos seleccionados para la propuesta son:

Dispositivo	Módulos	Uso	Ubicación
1 Router Cisco con IP software. Cisco 3640	- 3 módulos con un puerto Fast Ethernet, FX. (número de parte NM-1FE-FX) - Un modulo con 2 tarjetas slot WAN (2 WAN card slot network module, número de parte NM-2W)	Un modulo de fibra óptica por cada VLAN o segmento de LAN que queramos conmutar por medio de nuestro switch. El modulo de WAN interfase Card es el que recibirá nuestro enlace dedicado que llega de la FES Zaragoza, además tiene la posibilidad de recibir otro enlace por la misma tarjeta.	Edificio de mantenimiento.
2 Switches 3com SuperStack II 9300 con 12 puertos LX	Sin módulos extra	De acuerdo al número de hilos de fibra óptica necesitamos 13 puertos de fibra, (uno por cada edificio, más 3 puertos que ocupan los 3 hilos que llegaran del router para formar las 3 VLANs)	Edificio de mantenimiento.
1 switch 3com SuperStack II 1100 con 12 puertos	Un modulo de transiver a Coaxial, número de parte 3c1206-6	Este equipo ayudará a conmutar la red del Centro de Cómputo y el modulo es para unir la parte de cable coaxial.	Centro de Cómputo.

Tabla 9: Dispositivos seleccionados capa 3 para la implementación de la propuesta.

Los dispositivos mostrados en la tabla 9, son en los que se basa la propuesta de segmentación de la Red LAN de la ENEP Aragón, debido a su facilidad de implementación y administración.

3.3 Redes de Area Local Virtuales. (VLAN's)

Para la parte de la segmentación del tráfico, lo que propongo es la implementación de VLAN´s, sus siglas provienen en ingles de "Virtual Local Area Network", las cuales dividirán el tráfico en 3 partes, además por las características de los switches podemos filtrar los protocolos de una red a otra, dejando así por ejemplo el tráfico de Novell en un solo segmento de la red (IPX/SPX). Esto lo hace a través de unos métodos conocidos como el "Packet Filtering" y el "Packet identification", y el encargado de mantener esta configuración además de la comunicación correcta entre las distintas VLAN's no importando los tipos de LAN's en estas es el VTP[31].

Primero describiré lo que es una VLAN, así como su funcionamiento, implementación y características. Dando lugar al final a la configuración propuesta.

Una VLAN se encuentra conformada por un conjunto de dispositivos de red, los cuales funcionan de igual manera como lo hacen los de una LAN, pero con la diferencia de que las estaciones que constituyen la VLAN no necesariamente deberán estar ubicadas en el mismo segmento físico, en nuestro caso físicamente tenemos varios edificios que conforman una VLAN, además de pertenecer a la misma subred de direcciones IP. La VLAN básicamente es una subred definida por software y es considerada como un dominio de broadcast.

[31] VTP= VLAN Trunking Protocol, provee funciones de mapeo entre las redes y la configuración de la VLAN.

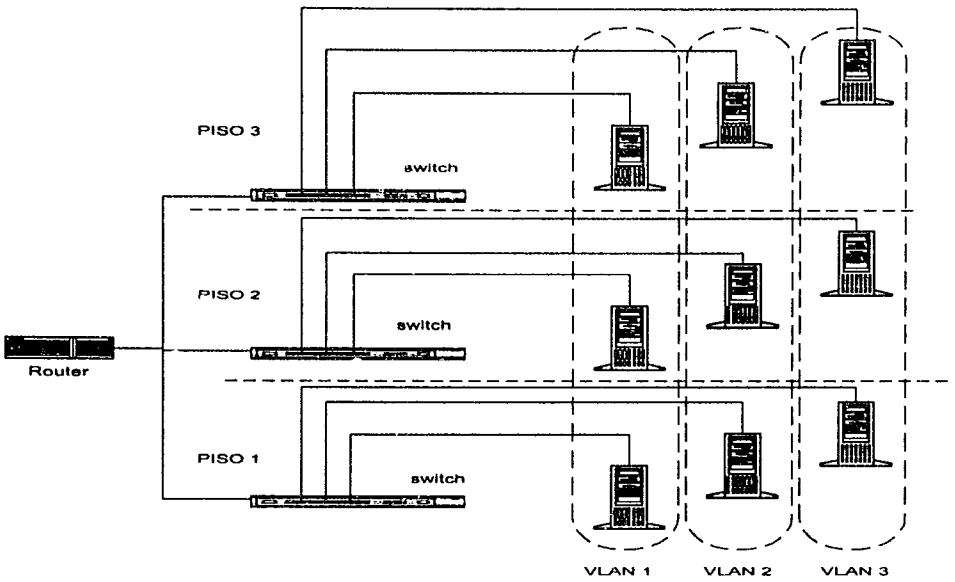


Figura 15. Esquema de General de una VLAN

Muchos fabricantes han tergiversado el concepto de lo que realmente es la red virtual; las cuales se implementan a través de switches, cada una con diferentes capacidades y limitaciones.

Unos de los términos más comunes cuando se define una VLAN es el *"Packet Filtering"*[32] y el *"Packet Identification"*[33] ya que son la manera en la se puede identificar y segmentar el tráfico de la red. El filtrado de paquetes es una técnica que examina la información de cada paquete con base a lo que el usuario definió. La Identificación de un paquete no es otra cosa que el etiquetado a cada paquete, ambas técnicas examinan el paquete cuando es enviado y recibido por lo switches. De acuerdo a las reglas que el administrador define estas reglas deciden la dirección de cada paquete, es decir su ubicación, tiempo de vida, y por supuesto alcance, esto se hace con el software que el propio switch trae directamente de fabrica.

El concepto de filtrado de paquetes es muy parecido al concepto usado por los ruteadores. Una etapa del filtrado se desarrolla en cada switch, lo que provee un control administrativo muy alto debido a que puede examinar muchos atributos de cada paquete, parte importante de mi propuesta debido a que de esta manera se podría segmentar el tráfico al analizar un paquete. De esta forma podemos agrupar usuarios basándonos en el número MAC y/o tipo de aplicaciones, como tráfico de Novell (IPX), Windows (NETBEUI), UNIX e Internet (TCP/IP) u otros que vallan apareciendo.

[32] Packet Filtering = Filtrado de paquetes.
[33] Packet Identification = Identificación de paquetes.

El switch compara una tabla de direcciones MAC utilizando el filtrado de paquetes, para así tomar una decisión en base a la entradas que el administrador le configure, de esta manera decide a donde enviar que paquetes. El filtrado de paquetes produce un nivel extra de procesamiento al switch antes de enviar cada paquete a otro puerto u a otro switch dentro de la red, esto puede producir efectos de latencia y mayor administración, sin embargo son costos que deben afrontarse debido a que considero que siempre debe existir alguien que administre y tome decisiones en cuestión de desempeño de una red, cualquier propuesta tiene pros y contras que se deben conocer.

La identificación de paquetes es un concepto relativamente nuevo, cuya principal función es la comunicación entre switches. Ésta técnica pone un identificador único en la cabecera del paquete para que después el paquete sea enviado a otro switch e identificado por este. Cuando el paquete es analizado e identificado por el switch, esté le quita el identificador antes de que sea trasmitido a una terminal final. Por lo tanto los beneficios que nos otorgan ambas técnicas son entre otros, que permiten a las arquitecturas VLAN la comunicación integral entre las LAN existentes así como la facilidad de comunicación entre distintos tipos de LAN, que en nuestro caso no se da, pero sin embargo en un futuro se puede contemplar migrar de tecnología si es necesario, estos cambios serían relativamente mucho más sencillos.

Ya que se conocen estas técnicas tan importantes dentro del concepto de una VLAN, debemos de conocer quien es el encargo de realizar estos procedimientos, de llevar a cabo dichas técnicas, este es el VTP (VLAN Trunking Protocol), el VTP es el encargado de proveer las funciones de mapeo de las dos técnicas anteriores, y además mantiene eficazmente la configuración de las VLAN en nuestras redes. Controla la creación, borrado y el cambio de nombres de las VLAN's, sin una intervención manual en cada switch, el protocolo detecta estos cambios y los distribuye a cada unos de los routers y switch de nuestra red.

Cuando un nuevo dispositivo es agregado a la red, este recibe mensajes del VTP y es configurado de manera automática dentro de las VLAN's existentes. Esto lo hace enviando avisos dentro de los frames hacia los dispositivos configurados con este protocolo, es decir a cada unos de los dispositivos vecinos. Este aviso contiene información referente al dominio de administración en el cual se encuentra el dispositivo, el número de revisión de la configuración, de esta manera los dispositivos vecinos aprenden la nueva configuración, lo que nos permite hacer los cambios solo en un dominio.

Características

- Los usuarios de las redes virtuales pueden ser distribuidos a través de una red LAN, incluso situándose en distintos concentradores de la misma red.

- Al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos se logra, como consecuencia directa, el incremento del ancho de banda en dicho grupo de usuarios, la posibilidad de situar bridges y routers entre ellos separando segmentos con diferentes tecnologías y protocolos. Es así como podemos separar el tráfico de protocolos como TCP/IP de IPX. Y mantenerlo es un segmento de la red.

- Las redes virtuales permiten que la ubicación geográfica no se limite a diferentes concentradores o plantas de un mismo edificio, sino a diferentes oficinas intercomunicadas mediante redes WAN o MAN, a lo largo de países y continentes sin ninguna limitación, mas la que impone el administrador de dichas redes. Esta característica podría ser utilizada en un futuro pero no es el fin de nuestra propuesta.

Tecnologías de switcheo.

Generalmente el switcheo tiende a aliviar la congestión producida por Ethernet, Token Ring y FDDI (Fiber Distributed Data Interface) al reducir significativamente el tráfico de Broadcast, aumentando el ancho de banda útil. Están diseñados para operar con las arquitecturas existentes (Hubs), y pueden ser instalados con un mínimo de condiciones.

La tecnología de los Switches es muy similar a la tecnología de Bridge. En este caso, el Bridge se encarga de unir dos segmentos de red con diferente subcapa MAC, copiando tramas de un lado a otro, en caso que sea necesario, respetando el formato del encabezado de la misma.

Como los Bridges, los Switches conectan 2 segmentos de red de acuerdo a una tabla de direcciones MAC, para saber en que segmento transmitir la trama entrante.

Sobre Ethernet, se mejora la utilización del ancho de banda del medio de transmisión, al segmentar la red en dominios de colisión y selectivamente transmitir el tráfico presente al segmento adecuado.

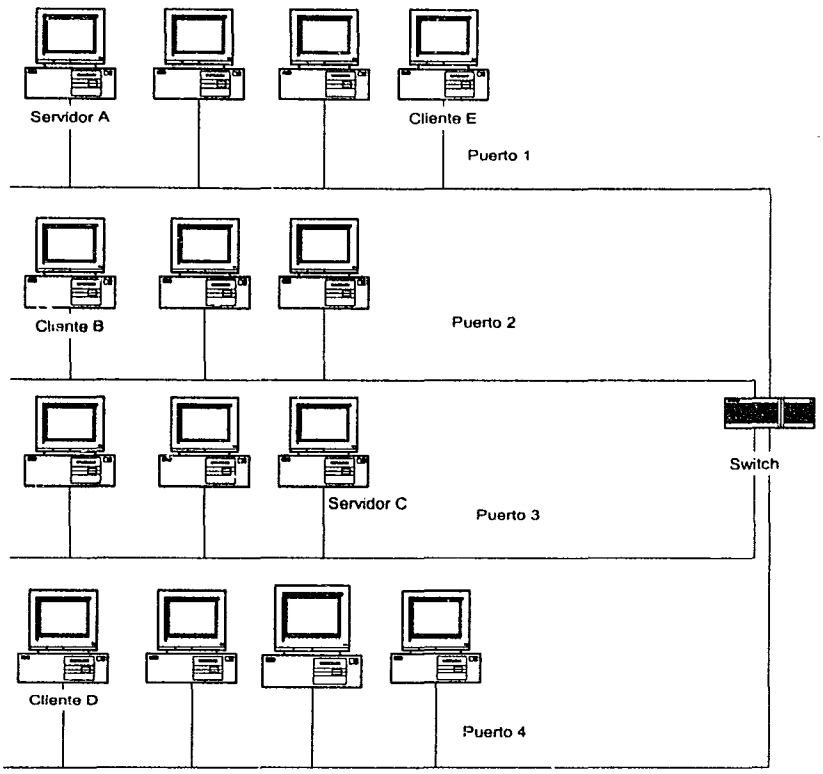


Figura 16. Funcionamiento de una VLAN.

De acuerdo a la figura 16 , el servidor A puede comunicarse con el cliente B, transmitiendo tramas desde el puerto 1 al 2; y, simultáneamente el servidor C puede comunicarse con el cliente D transmitiendo tramas desde el puerto 3 al 4. No se necesita pasar por el Switch, si se está en el mismo segmento.

Igualmente importante, los Routers son vitales para la tecnología de Switcheo, ya que de ellos depende la comunicación entre los grupos de trabajo definidos para cada VLAN. Además, proveen un acceso a recursos distribuidos, tales como servidores de correo, bases de datos y aplicaciones específicas; adicionalmente, conectan partes de la red que lógicamente están segmentadas de la manera tradicional y permiten un acceso remoto a través de enlaces WAN.

Los Switches de la figura 17 poseen la siguiente configuración, poseen un puerto de consola y 2 puertos con Fast Ethernet 100Mbps. Además, están distribuidos de tal manera que en cada slot se encuentran hasta 4 puertos, con un total de 5 slots. Entonces se tiene que, 2/2, es el 2 puerto del 2 slot. Estas son las configuraciones especificas de los switches en este ejemplo. La característica de modularidad le da gran versatilidad a las configuraciones de un switch, para la red LAN de la ENEP Aragón éstas pueden variar.

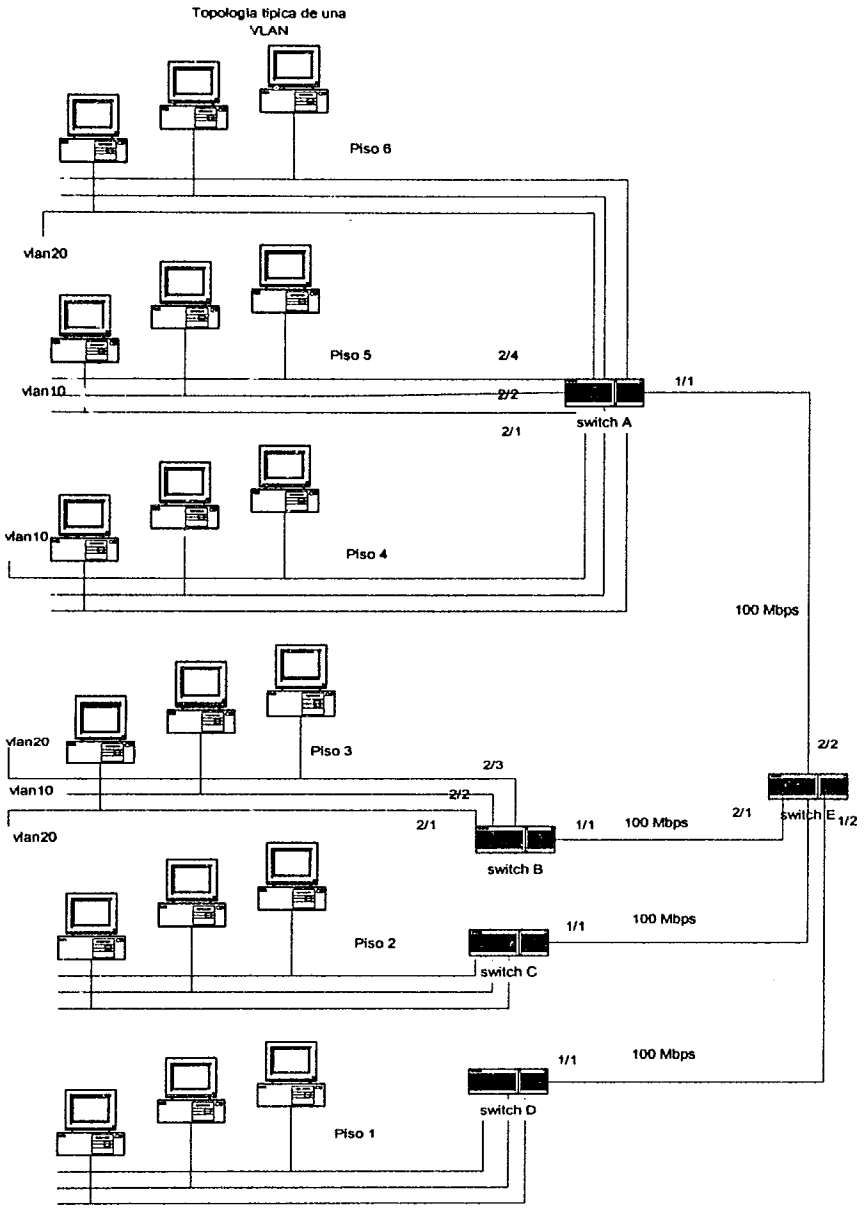


Figura 17. Funcionamiento de una VLAN.

El protocolo de comunicación el ISL (Inter Switch Link), aumenta una cabecera de 30 bytes. Se puede observar que la VLAN20 existe sobre el puerto 4 slot 2 del Switch A, puertos 3 y 1 slot 2 del Switch B y así con la VLAN10. VLAN10 y VLAN20 son solo nombres con los que se identificará cada una de las VLAN para este ejemplo.

Si en los puertos 3 o 1 del slot 2 en el Switch B, se produce una trama, el Switch B lo encapsula con una cabecera ISL y lo destina al Switch E, este a su vez verifica la cabecera para constatar que pertenece a la VLAN20, luego, lo evacua por el puerto 2/2 hacia el Switch A, este a su vez, remueve la cabecera ISL y verifica si el destino es multicast, broadcast o unicast.

Tipos de VLANs

Existen varias formas de definir una VLAN, las cuales se pueden dividir en 4 tipos generales como son:

- Basadas en agrupaciones por puertos.
- Basadas en direcciones MAC
- Basadas en la capa de red.
- Basadas en grupos multicast.

BASADAS EN AGRUPACIONES POR PUERTOS

En este caso se definen grupos de trabajo de acuerdo a agrupaciones de los puertos existentes en los Switches, es decir, puertos 1, 2, 3 pertenecen a la VLAN A y 4, 5 a la VLAN B. Esto inicialmente se implemento en un solo Switch, luego la segunda generación se oriento a realizarlo en múltiples Switches, en mi propuesta utilizaré este tipo de VLAN.

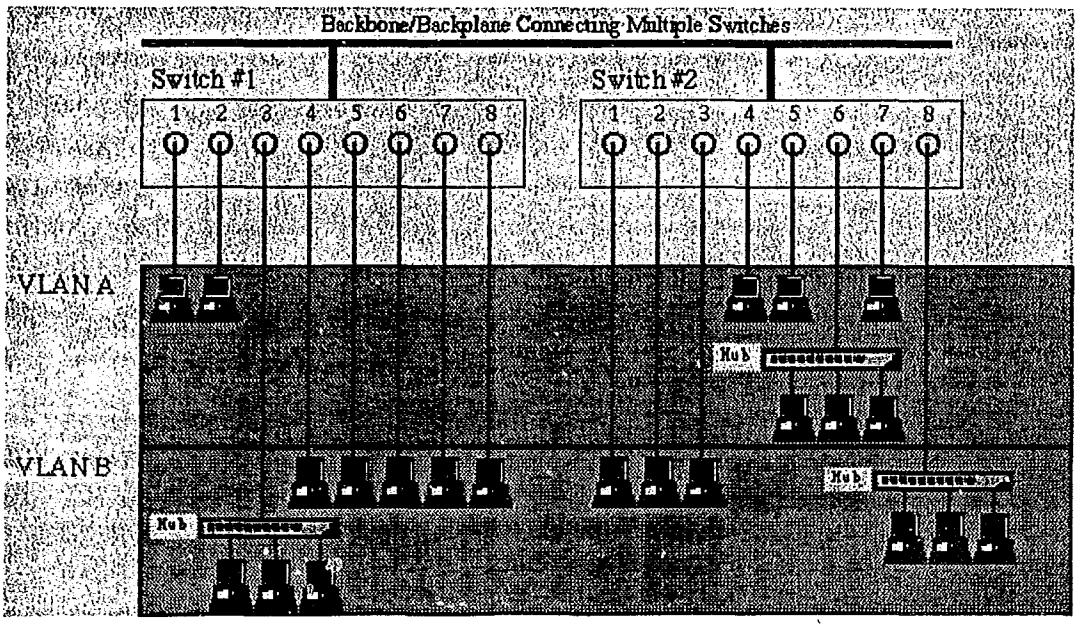


Figura 18. VLANS por puertos

Esta es la manera más común de definir los grupos de trabajo en una VLAN, su facilidad depende de la "inteligencia" de cada switch. Este tipo de VLAN's también conocidas como *VLAN's Estáticas* no son otras cosa que puertos de un switch que el administrador a asignado como parte de una VLAN Estática o por puertos, usando una aplicación de control de la VLAN que el fabricante del switch distribuye con la compra del dispositivo o configurándolo directamente dentro del switch. Estos puertos mantienen su configuración asignada hasta que el administrador de la red tome otra decisión. Aunque las VLAN's Estáticas requieren cambios por el administrador, este tipo de VLAN's son seguras debido a que se controla el tráfico deseado, además de ser fáciles de configurar y de monitorear.

Ventajas:

- Facilidad de movimientos y cambios.

Un movimiento supone que la estación cambia de ubicación física pero sigue perteneciendo a la misma VLAN. Requiere reconfiguración del puerto al que se conecta la estación salvo si se utilizan técnicas de asignación dinámica a VLAN. Un cambio implica pertenencia a una nueva VLAN sin movimiento físico. El puerto del conmutador ha de configurarse como perteneciente a la nueva VLAN y la estación puede precisar reconfiguración (por ejemplo si se utiliza protocolo IP sin servidor DHCP). La reconfiguración de la estación no será necesaria si la subred (IP, IPX, etc.) a la que pertenece esta totalmente contenida en la VLAN. Cualquier operación de añadir, mover o cambiar un usuario se traduce normalmente en la reconfiguración de un puerto y algunas aplicaciones gráficas de gestión de VLANs automatizan totalmente esta reasignación.

- Micro segmentación y reducción del dominio de broadcast.

Aunque los conmutadores permiten dividir la red en pequeños segmentos, el tráfico broadcast sigue afectando al rendimiento de las estaciones y se precisan routers o VLANs para aislar los dominios de broadcast. La definición de VLANs por puerto implica que el tráfico de broadcast de una VLAN no afecta a las estaciones en el resto de VLANs puesto que es siempre interno a la VLAN en la que se origina.

- Multiprotocolo.

La definición de VLANs por puerto es totalmente independiente del protocolo o protocolos utilizados en las estaciones. No existen pues limitaciones para protocolos de uso poco común como VINES, OSI, etc. o protocolos dinámicos como DHCP.

Desventajas:

Administración. Los movimientos y cambios implican normalmente una reasignación del puerto del conmutador a la VLAN a la que pertenece el usuario. Aunque las aplicaciones de gestión facilitan esta tarea es recomendable combinar dichas aplicaciones con mecanismos de asignación dinámica de VLAN de forma que se asignan los puertos a la VLAN en función de la dirección MAC o de otros criterios como la dirección de nivel 3. Cisco ha desarrollado un método de asignación dinámica de red VLAN a puerto basándose en las direcciones MAC de las estaciones de red.

BASADAS EN DIRECCIONES MAC

También conocidas como VLAN's Dinámicas y como su mismo nombre lo indica, se basan en la dirección Hardware presente en cada tarjeta de red de cada equipo, esto es, al nivel de la capa 2 del modelo OSI, específicamente en la subcapa MAC. Es decir, aprovechando que los Switchs operan con tablas de direcciones MAC, estas mismas tablas se pueden agrupar de tal manera que se puedan conformar grupos de trabajo y así crear una VLAN.

Ventajas:

- Esto permite que cualquier cambio de locación del equipo, no involucre un cambio de su configuración ni en la configuración de la red, de tal manera que se conserva su pertenencia a la misma VLAN.

- Multiprotocolo. No presenta ningún problema de compatibilidad con los diversos protocolos y soporta incluso la utilización de protocolos dinámicos tipo DHCP.

Desventajas:

- Un inconveniente se presenta cuando, por algún motivo falla la tarjeta de red del equipo, lo cual implica un cambio de la misma, es decir un cambio de la dirección MAC; esto hace que regularmente se actualizan las direcciones pertenecientes a determinada VLAN, aunque este inconveniente es poco común.

- Problemas de rendimiento y control de broadcast. Este método de definición de VLANs implica que en cada puerto del conmutador coexisten miembros de distintas

VLANs (se evita el problema si se utilizan puertos dedicados a estaciones pues cada puerto pertenecerá a una única VLAN) por lo que cualquier tráfico broadcast afecta al rendimiento de todas las estaciones. El tráfico multicast y broadcast se propaga por todas las VLANs.

- Complejidad en la administración. Todos los usuarios deben configurarse inicialmente en una VLAN. El administrador de la red introduce de forma manual, en la mayoría de los casos, todas las direcciones MAC de la red en algún tipo de base de datos. Cualquier cambio o nuevo usuario precisa modificación de la base de datos. Todo ello puede complicarse extremadamente en redes con un gran numero de usuarios o conmutadores. Existen soluciones alternativas para automatizar esta definición y normalmente se utiliza un servidor de configuración de forma que las direcciones MAC se copian de las tablas de direcciones de los conmutadores a la base de datos del servidor. La asignación dinámica de VLAN en base a dirección MAC es también posible si bien su implementación puede ser muy compleja.

BASADAS EN LA CAPA DE RED

En este caso, existen 2 posibilidades, primera basadas en direcciones IP, y segunda basadas en tipos de protocolos de la capa 3. De esta manera, desde el punto de vista del Switch, este inspecciona los números IP de las tramas que le llegan o simplemente sirve de puente entre las VLANs definidas para diferentes protocolos. No se lleva a cabo ningún tipo de ruteo o algo similar. Debido a esto, algunos proveedores incorporan cierta inteligencia a sus Switches adaptándolos con ciertas capacidades a nivel de la capa 3. Esto es, habilitándolos para tener funciones asociadas con el ruteo de paquetes.

Ventajas:

- Elimina la necesidad de la señalización entre Switches, ahorrando ancho de banda.

- Segmentación por protocolo. Es el método apropiado solo en aquellas redes en las que el criterio de agrupación de usuarios esté basado en el tipo de protocolo de nivel 3 y la segmentación física existente sea muy diferente a los patrones de direccionamiento.

- Asignación dinámica. Tanto la definición de VLAN's por dirección MAC como por protocolo de nivel 3 ayudan a automatizar la configuración del puerto del conmutador en una VLAN determinada.

Desventajas:

- Problemas de rendimiento y control de broadcast. La utilización de VLAN's de nivel 3 requiere complejas búsquedas en tablas de pertenencia que afectan al rendimiento global del conmutador. Los retardos de transmisión pueden aumentar entre un 50 y un 80 %. El problema de control de broadcast surge con las estaciones multiprotocolo o sistemas multistack (por ejemplo estaciones con stacks TCP/IP, IPX y AppleTalk) que pertenecen a tantas VLANs como protocolos utilizan y por lo tanto recibirán todos los broadcast provenientes de las diversas VLAN's en las que están incluidas.

- No soporta protocolos de nivel 2 ni protocolos dinámicos. La estación necesita una dirección de nivel 3 para que el conmutador la asigne a una VLAN. Las estaciones que utilicen protocolos de nivel 2 como NetBios y LAT no podrán asignarse a una VLAN. Si existen protocolos dinámicos como DHCP y la estación no tiene configurada su dirección IP ni su router por defecto el conmutador no puede clasificar la estación dentro de una VLAN. Una premisa esencial en la definición de VLAN's es que el rendimiento del conmutador no debe degradarse debido a la existencia de VLAN's. Las técnicas de marcado (identificación de paquetes pertenecientes a cada VLAN) utilizadas en la definición de VLAN's por puerto permiten mantener una velocidad de transmisión según el ancho de banda disponible (wire speed performance) y por ello ha prevalecido dicha solución en la definición del estándar 802.1Q. Estas técnicas permiten además la asignación de un mismo puerto o tarjeta de red a varias VLAN's (routers o servidores pueden aprovechar esta ventaja evitándose la utilización de tantos interfaces o tarjetas de red como VLANs). ISL (Inter-Switch Link) para Fast Ethernet/Token Ring y 802.10 para FDDI son dos ejemplos de técnicas de marcado.

BASADAS EN GRUPOS MULTICAST

En este caso lo que se tiene es un conjunto de direcciones IP, al cual le llegan paquetes vía Multicast, estos paquetes son enviados a direcciones proxy para que a partir de aquí se definan las direcciones IP que están autorizadas a recibir el paquete, esto se hace dinámicamente. Cada

estación de trabajo, obtiene la oportunidad de escoger un tipo particular de grupo con direcciones IP Multicast, respondiendo afirmativamente a la notificación tip o Broadcast. Esto se presta para que las VLAN trasciendan a conexiones al nivel de WAN's.

3.4 PROPUESTA DE SEGMENTACIÓN PARA LA RED LAN DE LA ENEP ARAGÓN

Después de que mencioné los distintos tipos de VLAN's puedo decir que mi propuesta se basa en una VLAN basada en agrupaciones por puerto, siendo así, la implementación quedaría como se muestra en el la figura 19.

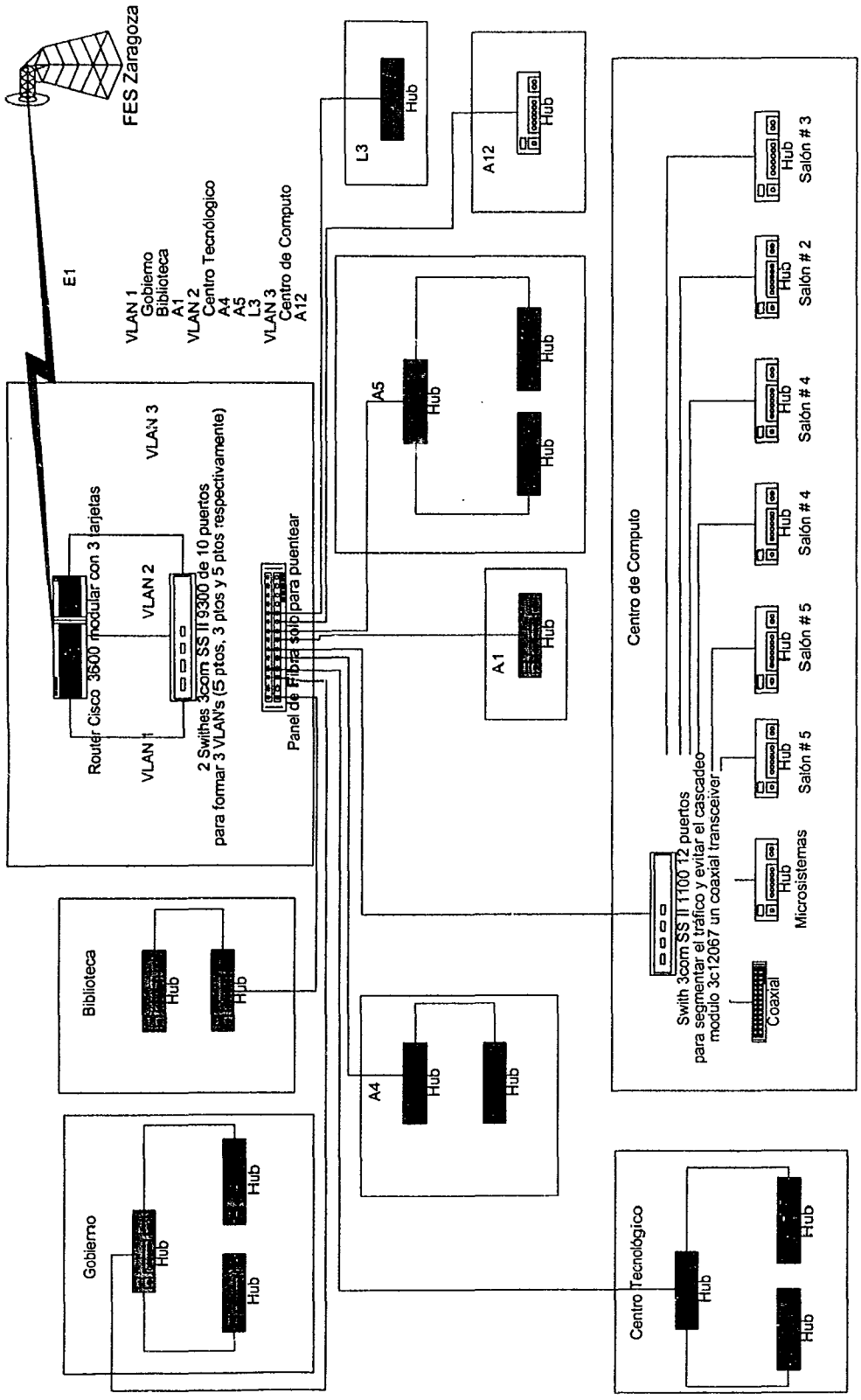


Figura 19. Propuesta de Segmentación para la Red LAN de la ENEP Aragón

En la figura 19 se puede observar la segmentación en tres VLAN's, cada VLAN corresponde a un segmento de red asignado a la ENEP Aragón, esto para una más fácil administración. Esto segmentos son lo que se analizaron en el capitulo 2. De echo esta configuración es la más básica que se puede implementar, ya que solamente me estoy basando la propuesta en estos segmentos, pero debido a las características de una VLAN sería relativamente sencillo cambiar un edificio de VLAN o incluso agregar otra VLAN. En tan solo un par de horas se puede cambiar la estructura completa de las VLAN`s.

La figura muestrá que del router salen 3 segmentos de fibra óptica, cada unos de estos segmentos le corresponde en un momento todo el ancho de banda del enlace dedicado E1 proveniente de la FES Zaragoza. Por las características del router propuesto, el cisco 3640, si es necesario se puede agregar otro modulo de fast ethernet para implementar una cuarta VLAN, es importante señalar que, por cada VLAN se necesita un modulo en el router y un puerto en el switch correspondiente.

Se tiene un bloque con 2 switches 9300, uno contendrá a la VLAN 1 y el segundo switch solo contendrá a la VLAN 2 y VLAN 3, de esta forma el tráfico entre VLAN's solo puede ser a través del router así cualquier señal de broadcast se mantienen en su propia VLAN, realmente como mencioné antes es una característica de las VLAN por puerto mantener las señales de broadcast en la VLAN en que fueron generadas. Por ejemplo, la señal de la impresora que se encuentra en el centro tecnológico (que se menciono en el capitulo 2) no tendría problemas de "Time out" debido a que su señal no saldría de la VLAN2, reduciendo así el tiempo de latencia en su propia red y a su vez el tráfico en el resto de la LAN.

Escogí tan solo dividir las VLAN's por los segmentos de red que actual,mente existen, ya que por el momento es una solución inmediata y puede facilitar la transacción del esquema actual sin segmentar hasta llegar a una red totalmente segmentada, sin embargo se puede dividir de acuerdo al tipo de servicios que prestan cada edificio dentro de la Red LAN, por ejemplo podemos dejar juntos en una VLAN al C.C.C.A, A4 y A5, ya que en estos edificios la principal tarea es el servicio a alumnos, como se mostró en el análisis del capitulo 2. También se puede dejar por ejemplo en una sola VLAN al edifico de Gobierno y A1 en una sola VLAN, ya que es un tráfico de información clasificada y no tiene por que ser vista por personas en edificio de biblioteca. Pero estos ejemplo son soluciones que se puede ir dando hasta el momento de centralizar la adminstración de la Red LAN en un solo departamento, como lo propondré en el siguiente capítulo.

El último switch que propongo es el ubicado en el C.C.C.A., con un modulo especial que nos ayudará a utilizar la tecnología existente en algunas partes de la red, como es el cable coaxial. Es

un transiver que nos ayudará a enviar la señal por el switch. Resolviendo en gran medida el mayor cuello de botella de la Red LAN de la E.N.E.P. Aragón.

El panel de parche que se encuentra en el la figura 19 entre los switches del edifico de mantenimiento y el resto de la LAN es muy importante, aunque su función es solo un puente entre la F.O que llega de lo edificios hacia los switches, nos facilita en gran medida el mantenimiento y cambio de edificios entre VLAN's

Por último en algunos casos los concentradores (hubs en la gráfica) son conectados en diferente forma a la tradicional, debido a las características técnicas de los concentradores de la E.N.E.P. se puede utilizar la configuración mostrada en la figura 19, disminuyendo un nivel de cascadeo en cada edificio en donde se aplica esta configuración. Tal es el caso del salón A504, Edificio de Gobierno y Centro Tecnológico. Ésta característica lo único que hace es cruzar internamente las señales recibidas por el cable UTP y así se tiene tres concentradores y solo un nivel de cascadeo, solo basta con oprimir el botón de "X over" que se encuentra en la parte trasera de los concentradores

Siendo así las ventajas que obtenemos por esta propuesta de segmentación mediante VLAN's son:

- Reducción de colisiones.
- Reducción de alcance en las señales de broadcast, debido a la microsegmentación.
- Reducción de tráfico en general.
- Fácil administración de la LAN.
- Se pueden implementar esquemas de seguridad.
- No se deja afuera ningún tipo de protocolo en las VLAN por puerto.
- Implementación de las bases para la generación a largo plazo de una red totalmente segmentada.
- Por las características de los switches descritas anteriormente la velocidad en cada punto aumentaría en gran medida.

CAPITULO 4.

Propuesta de administración y monitoreo para la Red de la ENEP Aragón

La propuesta del capítulo anterior seria inútil si después de todo la red de la ENEP Aragón no tuviera un control, una buena administración. Es por eso que mi trabajo no termina ahí, también propongo en primer lugar la creación de un departamento que unifique a los administradores de cada uno de los segmentos de red del campus. En otras palabras centralizar la administración en una área dedicada exclusivamente a la administración y monitoreo de la red de la ENEP Aragón; y en segundo lugar definiré algunas funciones y herramientas de monitoreo que pueden ser de utilidad.

En el mundo actual, en el que la informática gira en torno al concepto de red, el trabajo de los administradores de sistemas es muy complejo. Su misión consiste en mantener en funcionamiento recursos tales como routers, concentradores, servidores, así como cada dispositivo crítico que conforma la red.

Hay gran cantidad de motivos por los cuales un administrador necesita monitorear entre otros: la utilización del ancho de banda, el estado de funcionamiento de los enlaces, la detección de cuellos de botella, detectar y solventar problemas con el cableado, administrar la información de encaminamiento entre máquinas, etc. El monitoreo de la red es también un buen punto para comenzar con el estudio de los problemas de seguridad, por eso es importante el mantener la información disponible en cualquier momento de todos los dispositivos que conforman nuestra red. Por eso se propone la unificación de todos los administradores de la red de la ENEP Aragón en un solo departamento.

Este departamento de tener una mezcla de características como las de un NIC de la UNAM y un NOC de nuestra máxima casa de estudios, generando así sus propias funciones dentro de la ENEP Aragón, como lo seria el monitoreo del ancho de banda de las tres VLAN's que conforman la propuesta de segmentación de la red, generar una base de datos de las direcciones ip asignadas así como de direcciones MAC y su relación entre ambas, monitoreo de

uso de servidores importantes (ancho de banda que ocupan estos), mantenimiento de los elementos de la red como los concentradores y routers, eliminar problemas de cableado y comunicación de toda nuestra red, asignar direcciones IP a nuevas interfaces de red así como su instalación, generar políticas y procedimientos referentes a la utilización de la red de la ENEP Aragón. Estas son tan sólo una de las tareas, pero entre más se vaya adentrando este departamento, las funciones pueden ir creciendo debido a que de esta área dependerá en gran medida el funcionamiento de muchas actividades en el ENEP Aragón.

A continuación describiré las características de un NIC para darnos una idea a lo que me refiero con la mezcla de funciones.

4.1 El Network Information Center (NIC) de la UNAM.

El centro de información de la RedUNAM, mejor conocido como NIC, tiene como principal tarea el proveer información técnica y administrativa a los administradores de las diferentes dependencias que conforman nuestra Red, así como de establecer políticas y procedimientos para la óptima administración de las sub redes que conforman RedUNAM. Esta información la generaríamos nosotros mismos.

Este servicio es de gran ayuda ya que debemos tomar en cuenta de que la RedUNAM, por infraestructura, es la red académica más grande de Latino América. Alrededor de todo el Distrito Federal, área metropolitana, interior de la república y el extranjero, se encuentra toda nuestra red y hay que sumarle los enlaces a otras instituciones educativas, gubernamentales y privadas que hacen uso de nuestra RedUNAM. Debido a esto se crea una nueva necesidad, que es proveer de un buen servicio y atención a las necesidades de la RedUNAM.[32]

Todos estos aspectos requieren de una buena administración que permita optimizar los recursos de la red, así como satisfacer las necesidades de todos los usuarios, coordinar y delegar funciones a través de procedimientos y políticas de uso. Además de promover una cultura informática y de redes de computo, en estas tareas el NIC forma parte importante de dicha organización.

4.1.1 Funciones del NIC.

Las tareas más importantes del NIC son:

[32] Fuente: http://www.nic.unam.mx/

1. Mantenimiento y difusión de información.
2. Servicios.
3. Elaboración e implementación de políticas y procedimientos.
4. Eventos.
5. Presencia en organismos nacionales e internacionales.

1.- Mantenimiento y difusión de información; La RedUNAM es un conjunto de redes locales que cuentan con una parte administrativa, estos administradores locales (actualmente tenemos varios responsables, lo cual no es bueno) son los encargados de solucionar en primer instancia los problemas relacionados con su propia red y están sujetos a acatar los lineamientos establecidos por la DTD[33] de la DGSCA. Toda esta información se encuentra en una base de datos administrada por el NIC, quienes son los encargados de coordinar las actividades de toda la RedUNAM al establecer contacto con cada uno de los administradores de las redes de locales de cada dependencia. La información mantenida por el NIC es referente a:

- Contactos técnicos y administrativos.
- Segmentos de Red.
- Direcciones IP.
- Dominios.
- Tipos de enlaces.
- Hosts.

Además de esta información nosotros deberíamos contar con las direcciones MAC asociadas a cada una de nuestras direcciones IP asignadas en ese momento, para asi poder mantener una mejor ubicación de la direcciones IP, y así evitar colisiones por direcciones IP duplicadas.

También a través del los servicios de WWW y FTP del NIC, podemos consultar información concerniente a la Historia de RedUNAM, (de echo fue ahí de donde se consiguió parte la información mostrada en el capitulo uno en este trabajo) Internet, eventos, noticias, aspectos técnicos de la red, políticas, aplicaciones de Internet y solicitudes entre otros.

2.- Servicios; el NIC ofrece servicios relacionados a las necesidades generales de cada red local conectada a RedUNAM, como son:

[33] Dirección de Telecomunicaciones Digitales.

- *Servicios de Nombres.* Bajo la administración del NIC se encuentra lo que denominamos con DNS primario, el cual es una tabla de relación de direcciones IP con nombres por lo general asociado con el dominio UNAM.MX. Esto permite cada Hosts sea reconocido en Internet con un "Nombre" valido, cada máquina que necesite este servicio debe de estar dada de alta en la base de datos del DNS previa solicitud del administrador de la red local al NIC.
- *Asignación de direcciones IP.* El esquema de direccionamiento de la UNAM esta basado en direcciones IP, el NIC es el encargado de asignar segmentos o rangos de direcciones a cada dependencia, claro anteriormente el administrador de la red local debe hacer la solicitud al NIC. También el NIC se reserva el derecho de poder ceder o retirar la administración total o parcial de las subredes, si así lo considera pertinente buscando el mejor desempeño de la RedUNAM.
- *Asignación y solicitud de dominios.* Existen dos clases de asignación de nombres, las internas y la externas, para el caso de las internas es decir los nombres que contengan el subdominio UNAM.MX, el NIC se encarga de asignar el nombre es su DNS primario. Y para el caso de los dominios fuera de este subdominio es decir instituciones privadas por ejemplo, el NIC se encarga de hacer la petición del dominio ante el NIC México.
- *Servicios de servidores secundarios.* En ocasiones es necesario para ciertas instituciones ajenas a la UNAM conectadas a RedUNAM, el tener otro servidor para sus nombres, este servicio de Hosting lo provee también el NIC.
- *Conexión a RedUNAM.* Junto con el NOC el NIC, ofrece el servicio de conectar a instituciones que lo requieran a nuestra Red y así formar parte de Internet.
- *Capacitación.* El NIC coordina la mayor parte de las actividades en cuestión de capacitación dirigidas a los administradores de las redes locales de la Universidad.

Dentro de estos servicios nosotros podríamos prescindir el servicio de *Hosting* debido a que los servidores de la ENEP son solo locales y no tenemos algún servidor externo a la institución. Sin embargo podemos resumir la mayoría de estos servicios en la administración de nuestras propias direcciones IP.

3.- Elaboración e implementación de políticas y procedimientos. Para ayudarnos a la administración de redes, es necesario tener políticas y procedimientos para obtener un buen rendimiento de la red, siempre es necesario que exista una autoridad que las desarrolle e implemente, esta autoridad en la UNAM es el NIC. Las políticas internas de la ENEP Aragón deben de estar regidas también por una autoridad en constante comunicación con el NIC en DGSCA, y esa es el departamento que propongo.

4.- Eventos. El NIC coordinará eventos relacionados para difusión de los servicios de RedUNAM, aquí pueden ofrecerse seminarios o conferencias por parte del personal de dicho departamento que previamente debe estar capacitado con diferentes curso referentes a su tarea, la administración de la red local de la ENEP Aragón.

5.- Presencia en organismos nacionales e internacionales. El NIC forma parte de la organizaciones que se encargan de todo lo relacionado a Internet, como parte de la investigación y desarrollo en la Universidad. Constantemente debemos actualizarnos y un buen lugar en donde la investigación en la ingeniería en computación se desarrolle en la ENEP Aragón puede ser este departamento en donde los alumnos puedan formar parte, claro personal plenamente calificado debe estar al mando.

Ya tenemos definidas las tareas administrativas pero sin embargo también necesitamos definir algunas tareas como las que realiza el NOC[34] las cuales formarán parte de las tareas cotidianas dentro del departamento que propongo.

4.2 El Network Operation Center (NOC) de la UNAM.

Como todos los centros de operación del mundo, el Noc de la UNAM es el encargado de mantener funcionando de manera eficiente la interconexión de las redes locales, los enlaces de área amplia y la "columna vertebral" (backbone) de RedUNAM, es aquí en donde interactuará nuestro departamento trabajando en conjunto con el NOC de la UNAM, en primer lugar el departamento que propongo deberá resolver los problemas de interconexión dentro de la Red LAN de la ENEP Aragón y si el problema es de comunicación hacia fuera al resto de RedUNAM deberá comunicarse al NOC en DGSCA.

El NOC de la UNAM se ha dedicado a proporcionar apoyo a los administradores de redes locales para solucionar sus problemas de intercomunicación con otras redes, sin embargo en la ENEP Aragón actualmente se tienen que comunicar con por lo menos tres diferentes personas encargadas cada uno de un distinto punto de la Red LAN de la ENEP, lo que resta tiempo de respuesta a las acciones tomadas.[35]

El Centro de Operación también se encarga de estudiar el desempeño de la red y participar en las tareas de configuración, mantenimiento e implementación de las nuevas tecnologías en

[34] NOC: Network Operation Center
[35] Fuente: http://www.noc.unam.mx/

backbone de RedUNAM. Yo propondré unas herramientas que describiré más adelante, para la administración y constante monitoreo de los ancho de banda y colisiones en nuestra red LAN.

Las herramientas que pondré se llaman "Iris y MRTG".

4.2.1 Funciones del NOC.

El NOC de RedUNAM se encarga de detectar, coordinar y dar solución a las fallas que se pudieran presentar en algún sector de la red, pero es obvio que el tiempo de respuesta mejoraría considerablemente si tenemos un departamento encargado de hacer esto en la Red LAN de la ENEP Aragón y utilizar al NOC hasta un momento crítico.

En el momento que se detecta algún problema se deberá generar una alarma que será atendida por una o más personas que cuenten con los conocimientos técnicos de administración de redes, esto lo realizaremos con herramientas de monitoreo agregadonles shells que envíe correos o mensajes a radiolocalizadores por ejemplo.

Sin embargo también se realizan otras actividades en paralelo como son:

- Pruebas de equipos de red.
- Ruteo entre los dispositivos de nuestra red.
- Generación de boletines técnicos que surgen a partir de la experimentación con nuevos equipos y tecnologías de red.
- Tarificación del uso de la red.
- Mantenimientos.

Para desempeñar estos trabajos son necesarios algunas herramientas que discutiremos a continuación.

4.3 Herramientas de monitoreo.

La red local del la ENEP Aragón representa uno de los campos más importantes en la vida diaria en el campus, la habilidad para administrar esta LAN requiere del uso de ciertas herramientas, así del entendimiento de cómo estas herramientas funcionan y pueden darnos información necesaria para la toma de decisiones importantes en el mejoramiento de nuestra red. Una de las herramientas más importantes es el uso del SNMP[36] como parte de herramientas

[36] SNMP: "Simple Network Managment Protocol".

de monitoreo. En esta parte hablaré de su funcionamiento y de cómo una herramienta GNU[37] como lo es el MRTG[38].

4.3.1 ¿ Qué es SNMP ?

La respuesta a todas las necesidades antes expuestas, es el protocolo llamado Simple Network Management Protocol (SNMP). Diseñado en los años 80, su principal objetivo fue el integrar la administración de diferentes tipos de redes mediante un diseño sencillo y que produjera poca sobrecarga en la red.

SNMP opera en el nivel de aplicación, utilizando el protocolo de transporte TCP/IP, por lo que ignora los aspectos específicos del hardware sobre el que funciona. La gestión se lleva a cabo al nivel de IP, por lo que se pueden controlar dispositivos que estén conectados en cualquier red accesible desde la Internet, y no únicamente aquellos localizados en la propia red local. Evidentemente, si alguno de los dispositivos de encaminamiento con el dispositivo remoto a controlar no funciona correctamente, no será posible su monitorización ni reconfiguración.

El protocolo SNMP está compuesto por dos elementos: el agente (agent), y el gestor (manager). Es una arquitectura cliente-servidor, en la cual el agente desempeña el papel de servidor y el gestor hace el de cliente.

El agente es un programa que ha de ejecutase en cada nodo de red que se desea administrar o monitorizar. Ofrece un interfaz de todos los elementos que se pueden configurar. Estos elementos se almacenan en unas estructuras de datos llamadas "Management Information Base" (MIB), se explicarán más adelante. Representa la parte del servidor, en la medida que tiene la información que se desea administrar y espera comandos por parte del cliente.

El gestor es el software que se ejecuta en la estación encargada de monitorizar la red, y su tarea consiste en consultar los diferentes agentes que se encuentran en los nodos de la red los datos que estos han ido obteniendo.

Hay un comando especial en SNMP, llamado trap, que permite a un agente enviar datos que no han sido solicitados de forma explícita al gestor, para informar de eventos tales como: errores, fallos en la alimentación eléctrica, etc.

---

[37] GNU: "GNU is not UNIX", fundación que organiza licencias como la GPL "General Public License" que afecta a sistemas operativos como Linux u OpenBSD. Y algunos productos como Apache o Sendmail.
[38] MRTG: "Multi Router Traffic Grapher", Herramienta de monitoreo que usa SNMP, bajo licencias tipo GNU.

En esencia, el SNMP es un protocolo muy sencillo puesto que todas las operaciones se realizan bajo el paradigma de carga-y-almacenamiento (load-and-store), lo que permite un juego de comandos reducido. Un gestor puede realizar sólo dos tipos diferentes de operaciones sobre un agente: leer o escribir un valor de una variable en el MIB del agente. Estas dos operaciones se conocen como petición-de-lectura (get-request) y petición-de-escritura (set-request). Hay un comando para responder a una petición-de-lectura llamado respuesta-de-lectura (get-response), que es utilizado únicamente por el agente.

La posibilidad de ampliación del protocolo está directamente relacionado con la capacidad del MIB de almacenar nuevos elementos. Si un fabricante quiere añadir un nuevo comando a un dispositivo, como puede ser un router, tan sólo tiene que añadir las variables correspondientes a su base de datos (MIB).

Casi todos los fabricantes implementan versiones agente de SNMP en sus dispositivos: routers, concentradores, sistemas operativos, etc.

4.3.2 La cuestión de la seguridad

SNMP ofrece muy poco soporte para la autentificación. Tan sólo ofrece el esquema de dos palabras clave (two-passwords). La clave pública permite a los gestores realizar peticiones de valores de variables, mientras que la clave privada permite realizar peticiones de escritura. A estas palabras clave se les llama en SNMP "communities"

Cada dispositivo conectado con una red gestionada con SNMP, ha de tener configuradas estas dos communities.

Es muy común tener asignando por defecto el valor "public" al community público, y "private" al privado. Por lo que es muy importante cambiar estos valores para proteger la seguridad de la red.

4.3.3 ¿ Qué es el MIB ?

SNMP define un estándar separado para los datos gestionados por el protocolo. Este estándar define los datos mantenidos por un dispositivo de red, así como las operaciones que están permitidas. Los datos están estructurados en forma de árbol; en el que sólo hay un camino desde la raíz hasta cada variable. Esta estructura en árbol se llama Management Information Base (MIB) y se puede encontrar información sobre ella en varios RFC's.

En esencia, el SNMP es un protocolo muy sencillo puesto que todas las operaciones se realizan bajo el paradigma de carga-y-almacenamiento (load-and-store), lo que permite un juego de comandos reducido. Un gestor puede realizar sólo dos tipos diferentes de operaciones sobre un agente: leer o escribir un valor de una variable en el MIB del agente. Estas dos operaciones se conocen como petición-de-lectura (get-request) y petición-de-escritura (set-request). Hay un comando para responder a una petición-de-lectura llamado respuesta-de-lectura (get-response), que es utilizado únicamente por el agente.

La posibilidad de ampliación del protocolo está directamente relacionado con la capacidad del MIB de almacenar nuevos elementos. Si un fabricante quiere añadir un nuevo comando a un dispositivo, como puede ser un router, tan sólo tiene que añadir las variables correspondientes a su base de datos (MIB).

Casi todos los fabricantes implementan versiones agente de SNMP en sus dispositivos: routers, concentradores, sistemas operativos, etc.

4.3.2 La cuestión de la seguridad

SNMP ofrece muy poco soporte para la autentificación. Tan sólo ofrece el esquema de dos palabras clave (two-passwords). La clave pública permite a los gestores realizar peticiones de valores de variables, mientras que la clave privada permite realizar peticiones de escritura. A estas palabras clave se les llama en SNMP "communities"

Cada dispositivo conectado con una red gestionada con SNMP, ha de tener configuradas estas dos communities.

Es muy común tener asignando por defecto el valor "public" al community público, y "private" al privado. Por lo que es muy importante cambiar estos valores para proteger la seguridad de la red.

4.3.3 ¿ Qué es el MIB ?

SNMP define un estándar separado para los datos gestionados por el protocolo. Este estándar define los datos mantenidos por un dispositivo de red, así como las operaciones que están permitidas. Los datos están estructurados en forma de árbol; en el que sólo hay un camino desde la raíz hasta cada variable. Esta estructura en árbol se llama Management Information Base (MIB) y se puede encontrar información sobre ella en varios RFC's.

La versión actual de TCP/IP MIB es la 2 (MIB-II) y se encuentra definida en el RFC-1213. En ella se divide la información que un dispositivo debe mantener en ocho categorías (ver Tabla siguiente). Cualquier variable ha de estar en una de estas categorías.

Categoría	Información
System	Información del host del sistema de encaminamiento.
Interfaces	Información de las interfaces de red.
Addr-translation	Información de traducción de direcciones.
Ip	Información sobre el protocolo IP.
Icmp	Información sobre el protocolo ICMP.
Tcp	Información sobre el protocolo TCP.
Udp	Información sobre el protocolo UDP.
Egp	Información sobre el protocolo (exterior Gateway).

Tabla 10. Categorías TCP/IP

La definición de un elemento concreto MIB implica la especificación del tipo de dato que puede contener. Normalmente, los elementos de un MIB son enteros, pero también pueden almacenar cadenas de caracteres o estructuras más complejas como tablas. A los elementos de un MIB se les llama "objetos". Los objetos son los nodos hoja del árbol MIB, si bien, un objeto puede tener más de una instancia, como por ejemplo un objeto tabla. Para referirse al valor contenido en un objeto, se ha de añadir el número de la instancia. Cuando sólo exista una instancia del objeto, está es la instancia cero.

Por ejemplo, el objeto ifNumber de la categoría "interfaces" es un entero que representa el número de interfaces presentes en el dispositivo; mientras el objeto ipRoutingTable de la categoría "ip" contiene la tabla de encaminamiento del dispositivo.

Hay que acordarse de utilizar el número de la instancia para leer el valor de un objeto. En este caso, el número de interfaces presentes en un ruteador puede ser observado mediante la instancia ifNumber.0.

En el caso de ser un objeto tabla, se ha de utilizar el índice a la tabla como último número para especificar la instancia (fila de la tabla).

Existe otro estándar que define e identifica las variables MIB, llamado "Structure of Management Information" (SMI). SMI especifica las variables MIB, éstas se declaran empleando un lenguaje formal ISO llamado ASN.1, que hace que tanto la forma como los contenidos de estas variables sean no ambiguos.

El espacio de nombres ISO (árbol) está situado dentro de un espacio de nombres junto con otros árboles de otros estándares de otras organizaciones. Dentro del espacio de nombres ISO hay una rama específica para la información MIB. Dentro de esta rama MIB, los objetos están a su vez jerarquizados en subárboles para los distintos protocolos y aplicaciones, de forma que esta información puede representarse unívocamente.

La figura siguiente muestra el espacio de nombres del MIB del TCP/IP, éste está situado justo bajo el espacio del IAB "mgmt". La jerarquía también especifica el número para cada nivel.

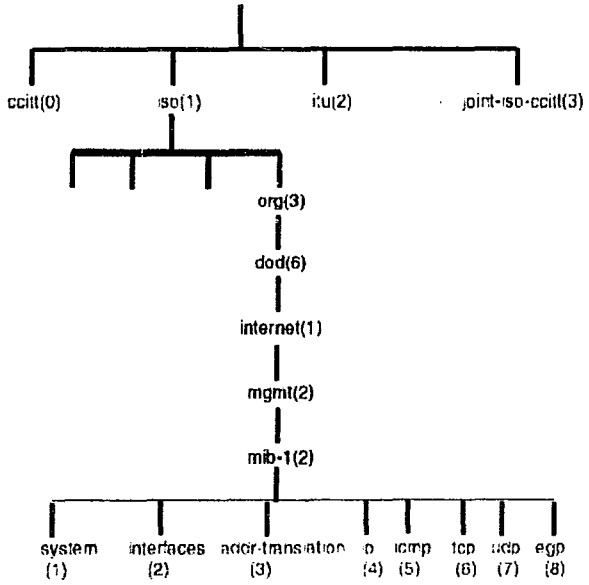


Figura 20. Árbol organizacional de TCP/IP

Es importante constatar que la mayor parte del software necesita el punto raíz (.) para localizar el objeto en el MIB. Si no se incluye el punto raíz, se asume que el path es relativo desde .iso.org.dod.internet.mgmt.mib-2.

De esta forma, el objeto ifNumber de la categoría "interfaces" se puede llamar:

.iso.org.dod.internet.mgmt.mib-2.interfaces.ifnumber

Existe otro estándar que define e identifica las variables MIB, llamado "Structure of Management Information" (SMI). SMI especifica las variables MIB, éstas se declaran empleando un lenguaje formal ISO llamado ASN.1, que hace que tanto la forma como los contenidos de estas variables sean no ambiguos.

El espacio de nombres ISO (árbol) está situado dentro de un espacio de nombres junto con otros árboles de otros estándares de otras organizaciones. Dentro del espacio de nombres ISO hay una rama específica para la información MIB. Dentro de esta rama MIB, los objetos están a su vez jerarquizados en subárboles para los distintos protocolos y aplicaciones, de forma que esta información puede representarse unívocamente.

La figura siguiente muestra el espacio de nombres del MIB del TCP/IP, éste está situado justo bajo el espacio del IAB "mgmt". La jerarquía también especifica el número para cada nivel.

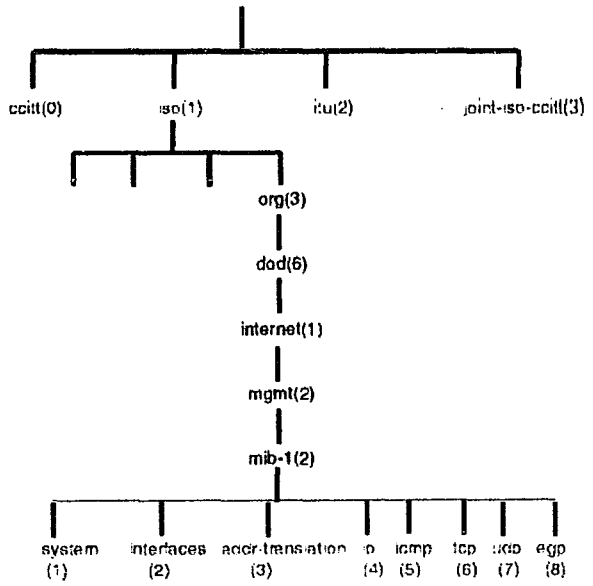


Figura 20. Árbol organizacional de TCP/IP

Es importante constatar que la mayor parte del software necesita el punto raíz (.) para localizar el objeto en el MIB. Si no se incluye el punto raíz, se asume que el path es relativo desde .iso.org.dod.internet.mgmt.mib-2.

De esta forma, el objeto ifNumber de la categoría "interfaces" se puede llamar:

.iso.org.dod.internet.mgmt.mib-2.interfaces.ifnumber

o el equivalente numérico:

.1.3.6.1.2.1.2.1

y la instancia es:

.iso.org.dod.internet.mgmt.mib-2.interfaces.ifnumber.0

o el equivalente numérico:

.1.3.6.1.2.1.2.1.0

Adicionales MIB se pueden añadir a este árbol conforme los vendedores definen nuevos objetos y publican los correspondientes RFC.

4.3.4 ¿ Cuál es el futuro de SNMP ?

Una nueva especificación llamada SNMPv2 está actualmente en rápido desarrollo. Esta versión trata de solucionar la laguna existente en cuestiones de seguridad del protocolo actual mediante mecanismos que se centran en la privacidad, la autentificación y el control de acceso. También permitirá un complejo mecanismo de especificación de variables, así como algunos comandos nuevos. El problema del SNMPv2 es que aún no es un estándar ampliamente aceptado, a diferencia del SNMPv1. No es fácil encontrar versiones de SNMPv2 de agentes ni de software que haga uso de los nuevos comandos. Dejemos que pase el tiempo y ya veremos que sucede en el futuro próximo.

4.4 El MRTG Multi Router Traffic Grapher

Ya que conocemos como funciona el SNMP, ahora como podemos utilizarlo para saber el rendimiento de nuestra red, para eso existen infinidad de programas que leen los datos del MIB, y nos lo presentan de una manera legible o simplemente son fáciles de utilizar, pero estos programas no deben representar una carga más para la red, uno de estos programa que además de ser muy bueno y de fácil configuración es el MRTG, es programa de libre distribución y que viene con el código fuente en C y en Perl, para modificarlo a nuestras necesidades. Este el programa que recomiendo para poder monitorear el ancho de banda utilizado para cada una de

las VLAN's propuestas en el capítulo anterior, simplemente se apunta a las interfaces que le dan la salida a cada una en el router del edificio de mantenimiento de la ENEP Aragón.

El MRTG es una herramienta que monitorea la carga de tráfico en los enlaces de redes. MRTG genera páginas HTML que contienen imágenes en formato PNG, anteriormente las generaba en formato GIF, pero por problemas legales con los derechos de autor del formato GIF, ahora se generan en este formato libre de este problema. Este programa proporciona una representación visual en tiempo real del tráfico. MRTG está basado en los lenguajes de programación Perl y C y trabaja bajo plataformas UNIX y Windows NT[39].

MRTG esta disponible bajo la licencia pública de GNU, GPL. Tiene un script escrito en perl que simula al gestor SNMP para leer los contadores de tráfico es decir el agente de SMTP de los routers y un rápido programa en C que registra los datos de tráfico y crea unas vistosas gráficas representando el tráfico sobre la conexión de red monitoreada. Estas gráficas están incrustadas dentro de páginas web que pueden ser vistas por cualquier browser.

El MRTG nos muestra también representaciones visuales de el tráfico visto durante los últimos siete días, las últimas cuatro semanas y los últimos doce meses. Esto es posible porque MRTG guarda un registro de todos los datos que han sido sacados de router. Este registro es automáticamente consolidado, así que no crece con el tiempo, pero aún contiene todos los datos relevantes de todo el tráfico visto durante los últimos dos años. Todo esto es ejecutado de una eficiente manera. Por lo tanto se pueden monitorear infinidad de enlaces de red desde cualquier máquina UNIX. Inclusive una PC con Linux, por lo que no requiere de una fuerte inversión, que podríamos de tachar como insignificante si tomamos en cuenta los alto precios de herramientas de marca, que no ofrecen exactamente lo mismo, y sin ser lo suficientemente modificables como lo es el MRTG.

Otra característica del MRTG es que no está limitado a monitorear el tráfico en la red, sin embargo, es posible monitorear alguna variable SNMP que se escoja. Se puede usar un programa externo escrito en C, Perl o Shell, que recoja los datos que tienen que ser monitoreados vía MRTG. Las personas en la red están usando MRTG para monitorear cosas como la carga de sistema o CPU, sesiones, módems disponibles y más. MRTG también le permite acumular dos o más fuentes de datos dentro de una gráfica particular.

Lo más relevante del MRTG

- Trabaja en la mayoría de las plataformas UNIX y Windows NT

[39] Fuente: http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/ y liga al software

- Utiliza Perl para una fácil configuración
- Tiene una implementación SNMP altamente portable escrita totalmente en Perl, gracias a Simon Leinen no es necesario instalar ningún paquete externo SNMP (gestor).
- Los archivos de registro del MRTG no crecen gracias al uso de un algoritmo único de consolidación de datos.
- MRTG viene una herramienta de configuración semiautomática.
- La máquina de consultas del MRTG inspecciona para reconfiguraciones de los puertos en el router y advierte al usuario cuando esto ocurre.
- Las rutinas de tiempo crítico están escritas en C gracias a la iniciativa de Dave Rand.
- Las gráficas son generadas directamente en formato GIF, usando la librería GD por Thomas Boutell.
- El aspecto de las página web producidas por el MRTG es altamente configurable.
  GNU esta disponible bajo la licencia pública GNU.

Un ejemplo de las gráficas mostradas por el MRTG es el siguiente:

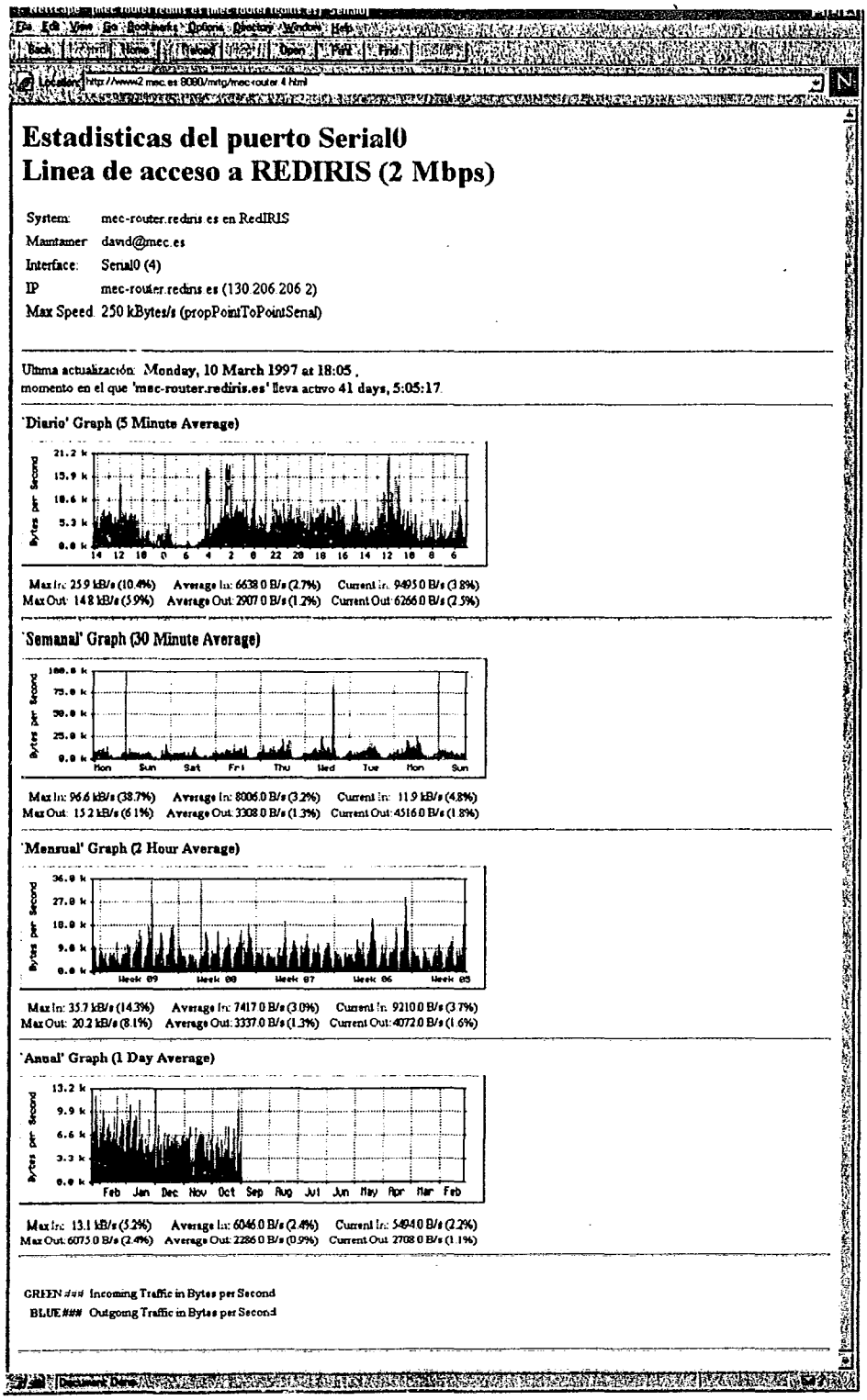


Figura 21. Gráficas realizadas por el MRTG

Esta herramienta es muy moldeable. Debido a que como hemos comentado está escrita en C y Perl, además de poder jalar scripts escritos en Shell, Perl o C para monitorear cualquier otra cosa que queramos, siempre y cuando estos script nos devuelvan los valores que queremos gráficar, en otras palabras, podemos utilizar esta herramienta como graficador de los datos más inusitados como temperatura, humedad, velocidad del viento, etc. Siempre y cuando podamos enviar los datos en el formato correcto al MRTG. Sin embargo esta herramienta debe ser complementada con algún otra que nos ayude con algunas tareas como el recabar una base de datos de las direcciones IP contra las direcciones MAC de un segmento, saber cuál es el uso real que le damos a nuestra red, tener un control de los paquetes que entran o salen de nuestros segmentos de red, este tipo de herramientas son los "Sniffers", investigando en la red, además de la experiencia que he tenido con respecto a estas herramientas puedo recomendar "Iris" un sniffer de "Eeye", del cual daré sus características a continuación.

4.5 IRIS "sniffer" para vigilar la red.

Lo primero que debemos comprender es ¿Qué es un Sniffer y cuales son sus características?, ¿Así cómo Iris en que trabaja?.

Analizar el trafico de una red o "husmear" es el proceso por el cual se monitorea el trafico entrante y saliente de una red, capturando y viendo de donde proviene cualquier teclazo de cualquier usuario.

Iris es un producto de "eeye.com", este es un analizador de tráfico y fue de los primeros en la red de este tipo de productos también conocidos como "sniffers", nos muestran el tráfico que fluye a través de nuestra red, y esta herramienta en particular es de fácil uso ya que con un simple click en un botón nos enseña gráficamente lo que sucede en la red.

La figura 22 muestra como el iris representa los paquetes que lee.

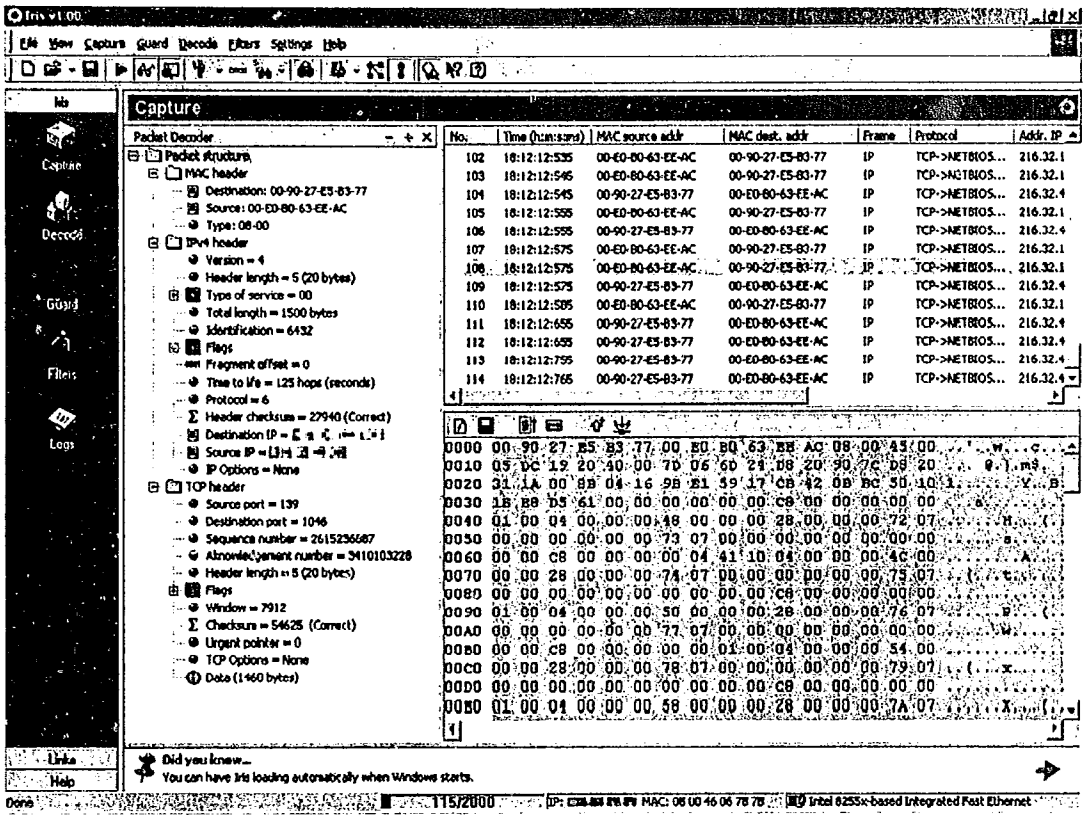


Figura 22. Representación de paquetes por parte del software "Iris"

Este tipos de herramientas nos permiten saber que entra y que sale de nuestra red, es un muy buen complemento de la herramienta anterior el MRTG, incluso podemos saber que está enviado y desde donde se está enviado, ya que no solo nos muestra una dirección Ip, si no también la dirección MAC de una tarjeta ethernet. Realmente es un buen perro guardián que nos ayudará a administrar el flujo de información.

Por la características anteriores puede ser una herramienta de monitoreo y administración de paquetes, sin embargo le podemos dar otras aplicaciones. Tomando esto encuesta el área dedicada a la administración de la red, si no cuenta con una base de datos de direcciones IP contra direcciones Mac, puede generar una con la ayuda de este software, pero eso no es todo también puede ser una herramienta de seguridad ya que literalmente puede reconstruir cada teclazo de un intento de intrusión a la red local. Teniendo de esta manera pruebas de un ataque a nuestra red.

Actualmente la versión de este software es la 2.0 pero no es un software GNU como en el caso del MRTG; debido a que es una empresa particular, su costo es de $1745 dólares con un

año de soporte, y los años subsecuentes de soporte tienen un valor de $550 dólares, el soporte incluye las actualizaciones de versiones asi como soporte via email o telefónico[40].

Las características principales de este producto son:

- Reconstrucción de paquetes.
- Manipulación de paquetes.
- Filtrar los paquetes por capa de red.
- Filtrar paquetes por capa de protocolo.
- Filtrar por palabras clave.
- Filtrar por dirección MAC.
- Filtrar por dirección IP.
- Filtrar por puerto.
- Reconstrucción de protocolos comunes.
- Bitácoras de paquetes reconstruidos, husmeados y conexiones foráneas a la red.

Iris reconstruye cada señal de una tecla presionada que entra o sale de la red, examinando la información critica para así poder representarla en forma gráfica haciéndola fácil de entender.

La figura 23 muestra el menu por el cual se puede seleccionar el tipo de filtro que se va a ocupar.

[40] Fuente: http://www.eeye.com/

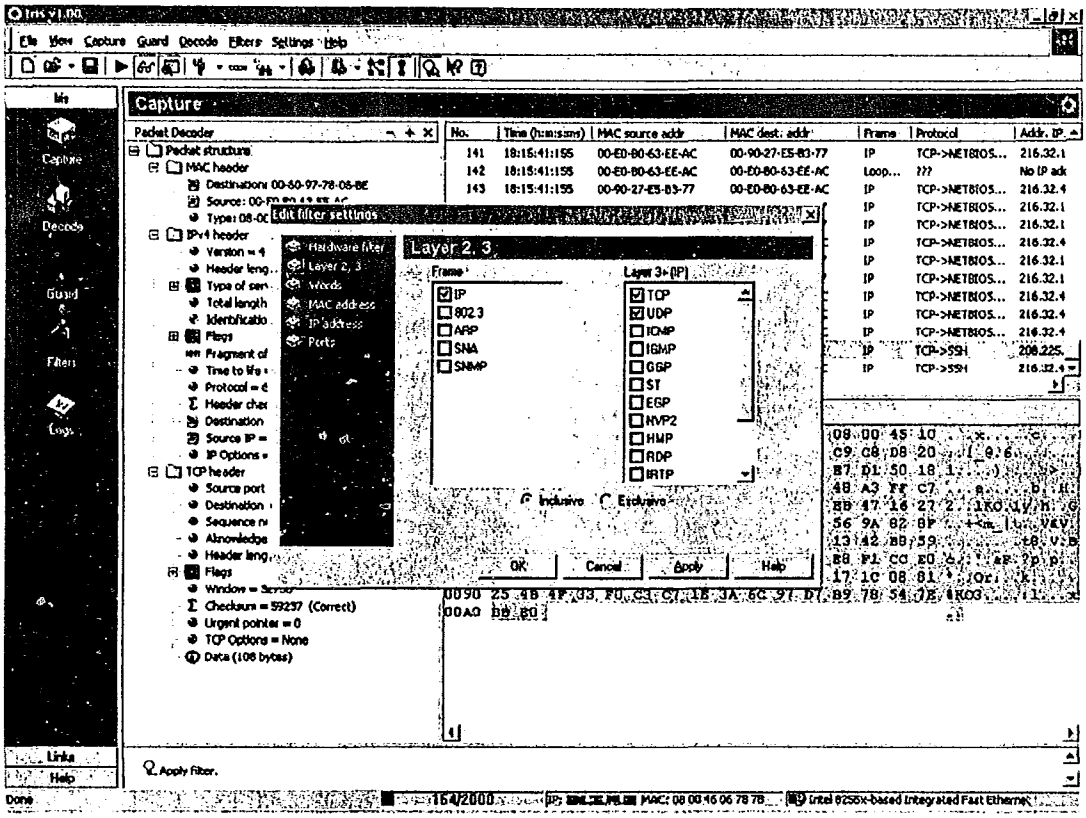


Figura 23. Menu de filtros del software "Iris"

Este sistema puede correr en máquinas con windows 95, 98, NT 4 o 2000, 32 MB de RAM, 1 Gb en D.D, Internet Explorer 4.01 o superior y al menos un procesador Pentium a 166 Mhz. Se puede bajar una versión de prueba de 30 días para evaluación del producto de la página.

http://www.eeye.com/

Como se mencionó anteriormente esta herramienta puede generar una base de datos de direcciones MAC, ya que al momento de estar generando su información también nos muestra la dirección MAC correspondiente a la dirección IP que esta "escuchando". De esta manera se podría avanzar en la administración de la Red LAN de la ENEP.

Si juntamos las características de un NIC, de un NOC, las herramientas propuestas, gente capacitada, información detallada de las configuraciones de la red. La generación de este departamento podría contemplar aproximadamente 4 personas, para el buen levantamiento de dicha información. Un jefe y tres técnicos que se encargaría de las tareas descritas en el

funcionamiento de un NIC y NOC, además se puede contemplar el uso de prestadores de servicio social, a los cuales se les capacitaría en el mismo departamento. Este departamento sería el encargado de implementar la propuesta de segmentación descrita en el capítulo 3, para estimar un tiempo de implementación es necesario realizar un plan de trabajo que no esta contemplado en este proyecto, sin embargo, el tiempo de implemetación y generación de la base de datos de direcciones MAC, junto con la generación de información detallada y actualizada de la red LAN de la ENEP Aragón, no debería pasar de 4 semanas con las personas antes mencionadas. De esta manera podrían comenzar las actividades del departamento sugerido en esta propuesta de administración.

Mientras, el MRTG podría dar información detallada del uso de las 3 VLAN's sugeridas en el capitulo 3, éste tendría que configurarse para que "leyera" los datos de las 3 interfaces del router sugerido, así el departamento de administración de la red LAN de la ENEP Aragón, podría tomar decisiones para cambiar o modificar las estructuras de las VLAN's, o sugerir en su caso, la compra de un nuevo enlace dedicado. Ya que se sabría exactamente cuanto ancho de banda se esta utilizando por área.

Queda así concluida la propuesta de administración de la Red LAN de la ENEP Aragón.

CONCLUSIONES.

Durante el desarrollo de este proyecto, he observado lo extenso que pueden ser los temas aquí tratados, tanto como para escribir tesis para cada uno de ellos por separado. Sin embargo, escogí a mi punto de vista lo más necesario para tener unas buenas bases de conocimiento previó y así comprender mejor mi propuesta.

Dentro de los detalles que encontré está el hecho de que la administración de una red es tan importante como la administración de un servidor, ahora bien una ley que podemos aplicar aquí es, entre más responsables existan menos orden vamos a encontrar en nuestra red. No puede haber muchos administradores que compartan al mismo grado la responsabilidad de esta tarea tan importante. Debe existir un solo administrador o departamento encargado de la administración de la red LAN, en una situación desordenada cada uno de los administradores pueden hacer perfectamente su trabajo pero si no existe un punto de comunicación o centralización de la información entre todos los administradores, difícilmente se tendrá un panorama completo de la situación real de una red LAN.

Esto es lo que sucedió en la ENEP Aragón, existen actualmente muchos responsables de la administración de la red LAN cada uno para un segmento de red, sin embargo es una sola entidad física, aunque existen diferentes segmentos de direcciones IP siguen siendo todos parte de una misma red, al haber tantas responsabilidades repartidas se ocasionó desinformación de la red LAN de la ENEP Aragón, es decir un administrador no conocía la situación en otro punto fuera de su administración, esto dió como resultado que no hubiera una persona o grupo de personas que supieran con exactitud la estructura física de la Red LAN de la ENEP Aragón. Esto fue visualizado durante el levantamiento de información y análisis del presente trabajo, ya que al entrevistar a los administradores de la red cada uno daba una versión diferente de la estructura general, cada uno tenia una visión diferente de lo que se debía hacer.

La desinformación se generó principalmente, en el momento en que estos segmentos de red fueron creciendo demasiado rápido, por lo tanto los cambios que un administrador realizaba con los pocos recursos que se le brindaban, en la mayoría de los casos no eran informados a los demás administradores; lo que generó un panorama erróneo de la situación de la red LAN de la ENEP Aragón.

Por esta razón pienso que en este caso es muy importante la centralización de responsabilidades en una sola persona o departamento, es decir un solo administrador para la red LAN de toda la ENEP Aragón, alguien que tenga bajo control todas las direcciones IP, las

direcciones MAC, monitoreo del ancho de banda, cambios de configuración, altas de nuevos segmentos, etc. En otras palabras la administración total en un solo departamento.

Se pueden implementar las etapas en la vida de un sistema en una red, como lo son el análisis, planeación, el diseño, la implementación, administración y las pruebas, de esta manera evitar el crecimiento descontrolado que puede ocasionar fallas como los cuellos de botella, colisiones, IP's duplicadas en una red. Por eso en este trabajo no solo trato de proponer una solución a un problema actual, si no también de hacer conciencia de que el análisis, la planeación, el diseño, la implementación, las pruebas y por supuesto la administración de una red LAN son de suma importancia para toda persona. Desde el administrador hasta el usuario final deben tomar conciencia de que hasta el mínimo programa utilizado genera una carga al rendimiento de la red LAN y por muy bueno que sea el análisis y el diseño de una red, si se descuida el mantenimiento y la administración, tarde o temprano la acumulación de estos pequeños programas pueden saturar el ancho de banda, por consiguiente disminuir el rendimiento (performance) de la red.

No hay que olvidar que el ancho de banda no deja de ser un recurso finito y algún día tiene que terminarse, incluso esta propuesta no puede tomarse como una solución final, debido a que siempre se necesitará más ancho de banda, más recursos para nuestros sistemas, dispositivos más poderosos, sin embargo esta propuesta de segmentación es muy flexible debido a la gran facilidad de ir implementando nuevas mejoras o ir creciendo la configuración implementando nuevos dispositivos, como lo podría ser la substitución de todos los concentradores (hub's) por switches eliminando así colisiones por completo, cambiando todas las tarjetas de red por "Fast Ethernet" aumentando de esta manera el ancho de banda para cada usuario final, la creación de una base de datos de las direcciones MAC localizando así la ubicación física de un dispositivo de red, en fin muchas configuraciones que a partir de la base que es esta propuesta, se pueden ir implementando; evitando con cada medida tomada la saturación de nuestro recurso más preciado el ancho de banda.

REFERENCIAS BIBLIOGRÁFICAS.

Gilbert Held, *LAN Managment with SNMP and RMON*, Wiley Computer Publishing, U.S.A.,1996.

Simson Garfinkel, *Seguridad Práctica en UNIX e Internet*,O'Reilly, México, 1999.

Hunt Craig, *TCP/IP Network Administration*, O'Reilly, U.S.A., 1998.

Terplan Kornerl, *Communication networks managemnt*, Prentice Hall, 1987.

Gari Novosel, *MCSE TCP/IP Exam Cram*, Microsoft, U.S.A., 1998.

Darril P. Black, *Managing Switched Local Area Networks*, Adisson Wesley, U.S.A. 1998.

Gilbert Held, *Virtual LAN's construction, implementation, and management*, Wiley Computer Publishing, U.S.A., 1997.

http://www.cisco.com/

http://www.3com.com/

http://www.eeye.com/

http://www.newbridge.com/

http://www.nmp.umt.edu/

http://www.cis.ohio-state.edu/

http://tonatiuh.uam.mx/

http://www.dgsca.unam.mx/

http://msdn.microsoft.com/

http://www.globetrotting.com/

http://www.nic.unam.mx/

http://www.noc.unam.mx/

http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/

http://www.linux-es.com/

http://net-snmp.sourceforge.net/