Universidad Austral de Chile
Facultad de Ciencias de la Ingeniería
Escuela de Electricidad y Electrónica

OPTIMIZACIÓN E IMPLEMENTACIÓN DE LA RED LAN DEL INSTITUTO DE ELECTRICIDAD Y ELECTRÓNICA UACH

Trabajo de Titulación para optar al Título de Ingeniero Electrónico

PROFESOR PATROCINANTE:
Sr. Pedro Rey Clericus
Ingeniero Electrónico

ESTEBAN ANDRÉS ASENJO CASTRUCCIO
VALDIVIA 2006

COMISIÓN DE TITULACIÓN

_____

Sr. Pedro Rey Clericus
Profesor Patrocinante

_____

Sr. Franklin Castro Rojas
Profesor Informante

_____

Sr. José Mardones Fernández
Profesor Informante

Fecha Examen de Titulación: 19 de mayo de 2006

AGRADECIMIENTOS

En memoria de mi padre, Aliro Asenjo V.

Un especial reconocimiento a los profesores del Instituto de Electricidad y Electrónica, quienes me apoyaron en los momentos difíciles y creyeron en mí, especialmente a don Pedro Rey y don Franklin Castro. También a Christian Lazo, del Instituto de Informática, quien me oriento e introdujo en el área de conectividad y que siempre tuvo la buena voluntad de atender mis consultas. Gracias a Luis Ampuero por su colaboración en la elaboración de este proyecto.

Gracias mamá y también a mi hermana Patty por el apoyo incondicional que me dieron. Misión Cumplida.

Gracias Denisse, siempre me diste ánimo y apoyo en los momentos difíciles.

A mis amigos con quienes la distancia no es motivo para estrechar fuertes lazos de amistad.

INDICE

INDICE DE FIGURAS

Página

INDICE DE TABLAS

RESUMEN

La presente Tesis de Pregrado, “Optimización e Implementación de la Red LAN del Instituto de Electricidad y Electrónica” tiene por objeto principalmente mejorar y optimizar los recursos existentes y también ser una herramienta para la docencia, investigación y incrementar el nivel educativo en el aprendizaje de los estudiantes de la carrera de Ingeniería Electrónica de la Universidad Austral de Chile.

En primera instancia en este trabajo de tesis se realiza una amplia introducción a las redes de datos y las tecnologías existentes actualmente, también se hace una descripción general de los dispositivos de red. Posteriormente, se analiza acuciosamente la Red UACh y específicamente la red del Instituto de Electricidad y Electrónica para descubrir sus debilidades y fortalezas. Finalmente se elabora un modelo nuevo de red, que es la base para lograr tener una red de transporte de datos ATM, que constituye el fin principal de este trabajo de tesis, pues la concretación de esta nueva red, permitiría tener una red alternativa, pero dedicada exclusivamente al desarrollo de la investigación, educación y mejoramiento de la calidad de los profesionales que egresan de las escuelas de la Facultad de Ciencias de la Ingeniería.

ABSTRACT

The present Thesis of Pregrado “Optimization and Implementation LAN Network of the Institute of Electricity and Electronic” intends in principle to improve and to optimize the existing resources and to be a tool for teaching, investigation and to increase the educative level in the learning of the Electronic Engineering students in the Universidad Austral de Chile.

In first instance of this thesis work is made an introduction to the existing networks and technologies at the moment, also makes a general description of the devices and equipment of networking. Later the UACh Network is analyzed diligently and specially the network of the Institute of Electricity and Electronic. All this to discover its weaknesses and strengths. Finally is elaborated a new model of network, that is the base to manage to have a network of transport of data ATM, that constitutes the main aim of this thesis work, because implementing this new network, to leave a network alternative, but dedicated exclusively to the development of investigation, education and improvement of the quality of the professionals who graduate from the schools of the Faculty of Engineering Sciences.

INTRODUCCIÓN GENERAL

El uso de ordenadores como herramienta de apoyo en el trabajo, es cada día más indispensable, pues permite realizar más tareas desde un solo lugar con mayor facilidad y en menor tiempo.

Estadísticas de la Subsecretaría de Telecomunicaciones hacen referencia a un aumento trimestral de un 12% en conexiones a Internet dedicadas en Chile, no dejando de lado los accesos conmutados analógicos, que sigue siendo la mayoría. Por otro lado, la cantidad de ordenadores en las distintas unidades de la Universidad Austral de Chile aumenta cada día más.

La tendencia anterior desencadena varios problemas, pues el aumento de estaciones de trabajo genera demanda de direcciones IP. Las direcciones IP versión 4 válidas en Internet son cada día mas escasas, por lo que se debe hacer uso de algún método para reutilizarlas. Por otro lado, el aumento del tráfico de paquetes en la red requiere implantar medidas de filtrado y seguridad.

Hoy en día se habla de Gigabit Ethernet como protocolo de acceso al medio. Sin embargo, no basta sólo con aumentar el ancho de banda, también se debe tener en cuenta otros puntos para obtener una red realmente eficiente.

Con el presente estudio se pretende optimizar el actual modelo de red existente en el Instituto de Electricidad y Electrónica de la Universidad Austral de Chile, estableciendo las consideraciones para su diseño y la creación de los cimientos para acceder a nuevas tecnologías.

La importancia de este estudio, no sólo reside en optimizar los recursos existentes de la red, sino también es crear una herramienta educativa para reforzar el aprendizaje de los estudiantes de Ingeniera Electrónica de la Universidad Austral de Chile en las áreas de redes y conectividad.

CAPITULO I : INTERNETWORKING

1.1 TERMINOLOGÍA DE NETWORKING

1.1.1 Redes de Datos

Las redes de datos se desarrollaron como consecuencia de aplicaciones comerciales diseñadas para microcomputadores. Por aquel entonces, los microcomputadores no estaban conectados entre sí como lo estaban los terminales de computadores mainframe, por ello no había una manera eficaz de compartir datos entre varios computadores. Se tornó evidente que el uso de disquetes para compartir datos no era un método eficaz, ni económico para desarrollar la actividad empresarial. Cada vez, que se modificaba un archivo, había que volver a compartirlo con el resto de sus usuarios. Si dos usuarios modificaban el archivo, y luego intentaban compartirlo, se perdía alguno de los dos conjuntos de modificaciones. Las empresas necesitaban una solución que resolviera con éxito los tres problemas siguientes:

- Cómo evitar la duplicación de equipos informáticos y de otros recursos.
- Cómo comunicarse con eficiencia.
- Cómo configurar y administrar una red.

Las empresas descubrieron que la tecnología de networking podía aumentar la productividad y ahorrar gastos. Las redes se agrandaron y extendieron casi con la misma rapidez con la que se lanzaban nuevas tecnologías y productos de red. A principios de la década de 1980 networking se expandió enormemente, aun cuando en sus inicios su desarrollo fue desorganizado. A mediados de la década de 1980, las tecnologías de red que habían emergido se habían creado con implementaciones de hardware y software distintas. Cada empresa dedicada a crear hardware y software para redes utilizaba sus propios estándares corporativos. Estos estándares individuales se desarrollaron como consecuencia de la competencia con otras empresas. Por lo tanto, muchas de las nuevas tecnologías no eran compatibles entre sí. Se volvió cada vez más difícil la comunicación entre redes que usaban distintas especificaciones. Esto a menudo obligaba a deshacerse de los equipos de la antigua red al implementar equipos de red nuevos.

Una de las primeras soluciones fue la creación de los estándares de red de área local (LAN - Local Area Network, en inglés). Como los estándares LAN proporcionaban un conjunto abierto de pautas para la creación de hardware y software de red, se podrían compatibilizar los equipos provenientes de diferentes empresas. Esto permitía la estabilidad en la implementación de las LAN. En un sistema LAN, cada departamento de la empresa era una especie de isla electrónica. A medida que el uso de los computadores en las empresas aumentaba, pronto resultó obvio que incluso las LAN no eran suficientes. Lo que se necesitaba era una forma de que la información se pudiera transferir rápidamente y con eficiencia, no solamente dentro de una misma empresa, sino también de una empresa a otra. La solución fue la creación de Redes de Área Metropolitana (MAN) y Redes de Área Extensa (WAN). Como las WAN podían conectar redes de usuarios dentro de áreas geográficas extensas, permitieron que las empresas se comunicaran entre sí a través de grandes distancias.

Distancia entre las CPU	Ubicación de las CPU	Nombre
0.1 m	Placa de circuito impreso/Asistente personal de datos	Motherboard Red de área personal (PAN)
1.0 m	Milímetro Mainframe	Red del sistema de la computadora
10 m	Habitación	Red de área local (LAN) Su aula
100 m	Edificio	Red de área local (LAN) Su escuela
1000 m = 1 km	Campus	Red de área local (LAN) Universidad de Stanford
100,000 m = 100 km	País	Red de área amplia (WAN) Cisco Systems, Inc.
1,000,000 m = 1,000 km	Continente	Red de área amplia (WAN) África
10,000,000 m = 10,000 km	Planeta	Wide Area Network (WAN) The Internet
100,000,000 m = 100,000 km	Earth-moon system	Red de área amplia (WAN) Tierra y satélites artificiales

Fig. 1.1 – Clasificación de las redes de acuerdo a la distancia

1.1.2 Dispositivos de red

Los equipos que se conectan de forma directa a un segmento de red se denominan dispositivos. Estos dispositivos se clasifican en dos grandes grupos. El primer grupo está compuesto por los dispositivos de usuario final. Los dispositivos de usuario final incluyen los computadores, impresoras, escáneres, y demás dispositivos que brindan servicios directamente

al usuario. El segundo grupo está formado por los dispositivos de red. Los dispositivos de red son todos aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación.

Los dispositivos de usuario final que conectan a los usuarios con la red también se conocen con el nombre de hosts. Estos dispositivos permiten a los usuarios compartir, crear y obtener información. Los dispositivos host pueden existir sin una red, pero sin la red las capacidades de los hosts se ven fuertemente limitadas. Los dispositivos host están físicamente conectados con los medios de red mediante una tarjeta de interfaz de red (NIC). Utilizan esta conexión para realizar las tareas de envío de correo electrónico, impresión de documentos, escaneado de imágenes o acceso a bases de datos.

Un NIC es una placa de circuito impreso que se coloca en la ranura de expansión de un bus de la placa madre de un computador, o puede ser un dispositivo periférico. También se denomina adaptador de red. Las NIC para computadores portátiles o de mano por lo general tienen el tamaño de una tarjeta PCMCIA. Cada NIC individual tiene un código único, denominado dirección de control de acceso al medio (MAC). Esta dirección se emplea para controlar la comunicación de datos para el host de la red. Tal como su nombre lo indica, la NIC controla el acceso del host al medio. No existen símbolos estandarizados para los dispositivos de usuario final en la industria de networking. Son similares en apariencia a los dispositivos reales para permitir su fácil identificación.

Fig. 1.2 – Dispositivos del usuario final

Los dispositivos de red son los que transportan los datos que deben transferirse entre dispositivos de usuario final. Los dispositivos de red proporcionan el tendido de las conexiones de cable, la concentración de conexiones, la conversión de los formatos de datos y la administración de transferencia de datos. Algunos ejemplos de dispositivos que ejecutan estas funciones son los repetidores, hubs, puentes, switches y routers. (Anexo A.2)

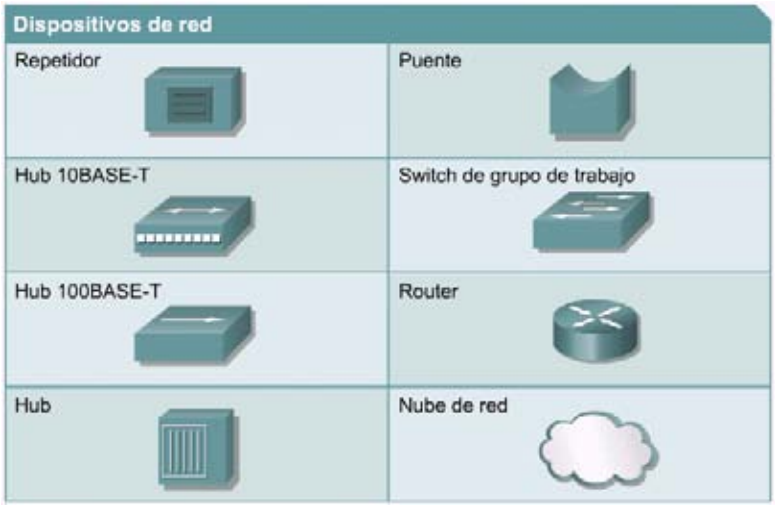

Fig. 1.3 – Dispositivos de red

1.1.3 Topologías de Red

La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios. La otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos.

Las topologías físicas generalmente usadas son las siguientes:

- Una *topología de bus* usa un solo cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este backbone.
- La *topología de anillo* conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.
- La *topología en estrella* conecta todos los cables con un punto central de concentración.

- Una *topología en estrella extendida* conecta estrellas individuales entre sí mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red.
- Una *topología jerárquica* es similar a una estrella extendida. Pero en lugar de conectar los hubs o switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.
- La *topología de malla* se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio. Como se puede observar en el gráfico, cada host tiene sus propias conexiones con los demás hosts. Aunque la Internet cuenta con múltiples rutas hacia cualquier ubicación, no adopta la topología de malla completa.

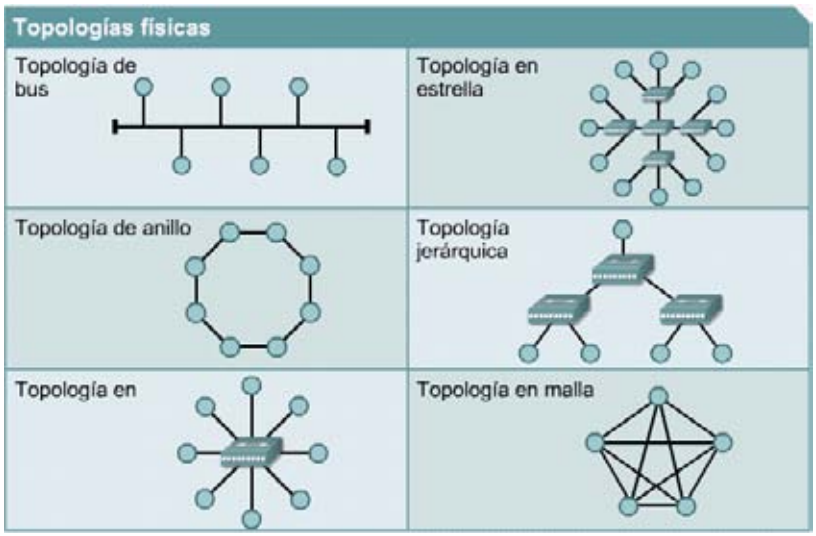

Fig. 1.4 – Topologías físicas

La topología lógica de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast y transmisión de tokens.

La topología broadcast significa que cada host envía sus datos hacia todos los demás hosts del medio de red. No existe una orden que las estaciones deban seguir para utilizar la red. Es por orden de llegada.

La segunda topología lógica es la transmisión de tokens. Esta controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial. Cuando un host recibe el token, ese host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token al siguiente host y el proceso se vuelve a repetir. Dos ejemplos de redes que utilizan la transmisión de tokens son Token Ring y la Interfaz de datos distribuida por fibra (FDDI).

1.1.4 Protocolos de Red

Los conjuntos de protocolos son colecciones de protocolos que posibilitan la comunicación de red desde un host, a través de la red, hacia otro host. Un protocolo es una descripción formal de un conjunto de reglas y convenciones que rigen un aspecto particular de cómo los dispositivos de una red se comunican entre sí. Los protocolos determinan el formato, la sincronización, la secuenciación y el control de errores en la comunicación de datos. Sin protocolos, el computador no puede armar o reconstruir el formato original del flujo de bits entrantes desde otro computador.

Los protocolos controlan todos los aspectos de la comunicación de datos, que incluye lo siguiente:

- Cómo se construye la red física.
- Cómo los computadores se conectan a la red.
- Cómo se formatean los datos para su transmisión.
- Cómo se envían los datos.
- Cómo se manejan los errores.

Estas normas de red son creadas y administradas por una serie de diferentes organizaciones y comités. Entre ellos se incluyen el Instituto de Ingeniería Eléctrica y Electrónica (IEEE), el Instituto Nacional Americano de Normalización (ANSI), la Asociación de la Industria de las Telecomunicaciones (TIA), la Asociación de Industrias Electrónicas (EIA) y la Unión Internacional de Telecomunicaciones (UIT), antiguamente conocida como el Comité Consultivo Internacional Telegráfico y Telefónico (CCITT).

1.1.5 Redes de Área Local

Las LAN constan de los siguientes componentes:

- Computadores.
- Tarjetas de interfaz de red.
- Dispositivos periféricos.
- Medios de networking.
- Dispositivos de networking.

Las LAN permiten a las empresas aplicar tecnología informática para compartir localmente archivos e impresoras de manera eficiente, y posibilitar las comunicaciones internas. Para ello conectan los datos, las comunicaciones locales y los equipos informáticos. Un buen ejemplo de esta tecnología es el correo electrónico.

Algunas de las tecnologías comunes de LAN son:

- Ethernet.
- Token Ring.
- FDDI.

1.1.6 Redes de Área Amplia

Las WAN interconectan las LAN, que a su vez proporcionan acceso a los computadores o a los servidores de archivos ubicados en otros lugares. Como las WAN conectan redes de usuarios dentro de un área geográfica extensa, permiten que las empresas se comuniquen entre sí, a través de grandes distancias. Las WAN permiten que los computadores, impresoras y otros dispositivos de una LAN cooperen y sean compartidas por redes en sitios distantes.

Las WAN proporcionan comunicaciones instantáneas a través de zonas geográficas extensas. El software de colaboración brinda acceso a información en tiempo real y recursos que permiten realizar reuniones entre personas separadas por largas distancias, en lugar de hacerlas en persona. Networking de área amplia también dio lugar a una nueva clase de

trabajadores, los empleados a distancia, que no tienen que salir de sus hogares para ir a trabajar.

Las WAN están diseñadas para realizar lo siguiente:

- Operar entre áreas geográficas extensas y distantes.
- Posibilitar capacidades de comunicación en tiempo real entre usuarios.
- Brindar recursos remotos de tiempo completo, conectados a los servicios locales.
- Brindar servicios de correo electrónico, World Wide Web, transferencia de archivos y comercio electrónico.

Algunas de las tecnologías comunes de WAN son:

- Módems.
- Red digital de servicios integrados (RDSI).
- Línea de suscripción digital (DSL - Digital Subscriber Line).
- Frame Relay.
- Series de portadoras para EE.UU. (T) y Europa (E): T1, E1, T3, E3.
- Red óptica síncrona (SONET).

1.1.7 Redes de Área Metropolitana

La MAN es una red que abarca un área metropolitana, como por ejemplo, una ciudad o una zona suburbana. Una MAN generalmente consta de una o más LAN dentro de un área geográfica común. Normalmente, se utiliza un proveedor de servicios para conectar dos o más sitios LAN utilizando líneas privadas de comunicación o servicios ópticos. También se puede crear una MAN usando tecnologías de puente inalámbrico enviando haces de luz a través de áreas públicas.

1.1.8 Redes de Área de Almacenamiento

Una SAN es una red dedicada de alto rendimiento, que se utiliza para trasladar datos entre servidores y recursos de almacenamiento. Al tratarse de una red separada y dedicada,

evita todo conflicto de tráfico entre clientes y servidores. La tecnología SAN permite conectividad de alta velocidad, de servidor a almacenamiento, reservas a almacenamiento, o servidor a servidor. Este método usa una infraestructura de red por separado, evitando así cualquier problema asociado con la conectividad de las redes existentes.

Las SAN poseen las siguientes características:

- **Rendimiento:** Las SAN permiten el acceso concurrente de matrices de disco o cinta por dos o más servidores a alta velocidad, proporcionando un mejor rendimiento del sistema.
- **Disponibilidad:** Las SAN tienen una tolerancia incorporada a los desastres, ya que se puede hacer una copia exacta de los datos mediante una SAN hasta una distancia de 10 kilómetros o 6,2 millas.
- **Escalabilidad:** Al igual que una LAN/WAN, puede usar una amplia gama de tecnologías. Esto permite la fácil reubicación de datos de copia de seguridad, operaciones, migración de archivos, y duplicación de datos entre sistemas.

1.1.9 Red Privada Virtual

Una VPN es una red privada que se construye dentro de una infraestructura de red pública, como la Internet global. Con una VPN, un empleado a distancia puede acceder a la red de la sede de la empresa a través de Internet, formando un túnel seguro entre el PC del empleado y un router VPN en la sede.

La VPN es un servicio que ofrece conectividad segura y confiable. Las VPN conservan las mismas políticas de seguridad y administración que una red privada. Son la forma más económica de establecer una conexión punto-a-punto entre usuarios remotos y la red de un cliente de la empresa. Los tres principales tipos de VPN se describen a continuación:

- **VPN de acceso:** Las VPN de acceso brindan acceso remoto a un trabajador móvil y una oficina pequeña/oficina hogareña (SOHO), a la sede de la red interna o externa, mediante una infraestructura compartida. Las VPN de acceso usan tecnologías analógicas, de acceso telefónico, RDSI, línea de suscripción digital (DSL), IP móvil y

de cable para brindar conexiones seguras a usuarios móviles, empleados a distancia y sucursales.

- **Redes internas VPN:** Las redes internas VPN conectan a las oficinas regionales y remotas a la sede de la red interna mediante una infraestructura compartida, utilizando conexiones dedicadas. Las redes internas VPN difieren de las redes externas VPN, ya que sólo permiten el acceso a empleados de la empresa.
- **Redes externas VPN:** Las redes externas VPN conectan a socios comerciales a la sede de la red mediante una infraestructura compartida, utilizando conexiones dedicadas. Las redes externas VPN difieren de las redes internas VPN, ya que permiten el acceso a usuarios que no pertenecen a la empresa.

1.1.10 Redes Internas y Externas

Una de las configuraciones comunes de una LAN es una red interna, a veces denominada "intranet". Los servidores de web de red interna son distintos de los servidores de web públicos, ya que es necesario que un usuario público cuente con los correspondientes permisos y contraseñas para acceder a la red interna de una organización. Las redes internas están diseñadas para permitir el acceso por usuarios con privilegios de acceso a la LAN interna de la organización. Dentro de una red interna, los servidores de web se instalan en la red. La tecnología de navegador se utiliza como interfaz común para acceder a la información, por ejemplo datos financieros o datos basados en texto y gráficos que se guardan en esos servidores.

Las redes externas hacen referencia a aplicaciones y servicios basados en la red interna, y utilizan un acceso extendido y seguro a usuarios o empresas externas Este acceso habitualmente se logra mediante contraseñas, identificaciones de usuarios, y seguridad a nivel de las aplicaciones. Por lo tanto, una red externa es la extensión de dos o más estrategias de red interna, con una interacción segura entre empresas participantes y sus respectivas redes internas.

1.2 ANCHO DE BANDA

El ancho de banda se define como la cantidad de información que puede fluir a través de una conexión de red en un período dado. Es esencial comprender el concepto de ancho de banda al estudiar networking, por las siguientes cuatro razones:

- El ancho de banda es finito.
- El ancho de banda no es gratuito.
- El ancho de banda es un factor clave a la hora de analizar el rendimiento de una red, diseñar nuevas redes y comprender la Internet.
- La demanda de ancho de banda no para de crecer.

El ancho de banda varía según el tipo de medio, además de las tecnologías LAN y WAN utilizadas. La física de los medios fundamenta algunas de las diferencias. Las señales se transmiten a través de cables de cobre de par trenzado, cables coaxiales, fibras ópticas, y por el aire. Las diferencias físicas en las formas en que se transmiten las señales son las que generan las limitaciones fundamentales en la capacidad que posee un medio dado para transportar información. No obstante, el verdadero ancho de banda de una red queda determinado por una combinación de los medios físicos y las tecnologías seleccionadas para señalizar y detectar señales de red.

El ancho de banda es la medida de la cantidad de información que puede atravesar la red en un período dado de tiempo.

La tasa de transferencia se refiere a la medida real del ancho de banda, en un momento dado del día, usando rutas de Internet específicas, y al transmitirse un conjunto específico de datos. Desafortunadamente, por varios motivos, la tasa de transferencia a menudo es mucho menor que el ancho de banda digital máximo posible del medio utilizado. A continuación se detallan algunos de los factores que determinan la tasa de transferencia:

- Dispositivos de Internetworking.
- Tipo de datos que se transfieren.
- Topología de la red.

- Cantidad de usuarios en la red.
- Computador del usuario.
- Computador servidor.
- Estado de la alimentación.

El ancho de banda teórico de una red es una consideración importante en el diseño de la red, porque el ancho de banda de la red jamás será mayor que los límites impuestos por los medios y las tecnologías de networking escogidos. No obstante, es igual de importante que un diseñador y administrador de redes considere los factores que pueden afectar la tasa de transferencia real. Al medir la tasa de transferencia regularmente, un administrador de red estará al tanto de los cambios en el rendimiento de la red y los cambios en las necesidades de los usuarios de la red. Así la red se podrá ajustar en consecuencia.

1.3 MODELOS DE NETWORKING

1.3.1 Uso de Capas para Describir la Comunicación de Datos

Los modelos OSI y TCP/IP se dividen en capas que explican cómo los datos se comunican de un computador a otro. Los modelos difieren en la cantidad y la función de las capas. No obstante, se puede usar cada modelo para ayudar a describir y brindar detalles sobre el flujo de información desde un origen a un destino.

Para que los paquetes de datos puedan viajar desde el origen hasta su destino a través de una red, es importante que todos los dispositivos de la red hablen el mismo lenguaje o protocolo. Un protocolo de comunicaciones de datos es un conjunto de normas, o un acuerdo, que determina el formato y la transmisión de datos.

Es importante recordar que los protocolos preparan datos en forma lineal. El protocolo en una capa realiza un conjunto determinado de operaciones sobre los datos al prepararlos para ser enviados a través de la red. Los datos luego pasan a la siguiente capa, donde otro protocolo realiza otro conjunto diferente de operaciones.

Una vez que el paquete llega a su destino, los protocolos deshacen la construcción del paquete que se armó en el extremo de origen. Esto se hace en orden inverso. Los protocolos para cada capa en el destino devuelven la información a su forma original, para que la aplicación pueda leer los datos correctamente.

1.3.2 Modelo OSI

Para enfrentar el problema de incompatibilidad de redes, la Organización Internacional de Normalización (ISO) investigó modelos de networking como la red de Digital Equipment Corporation (DECnet), la Arquitectura de Sistemas de Red (SNA) y TCP/IP a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. En base a esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes.

El modelo de referencia de Interconexión de Sistemas Abiertos (OSI) lanzado en 1984 fue el modelo de red descriptivo creado por ISO. Proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial.

El modelo de referencia OSI se ha convertido en el modelo principal para las comunicaciones por red. Aunque existen otros modelos, la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia de OSI. Además, se considera la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

1.3.2.1 Capas del Modelo OSI

El modelo de referencia OSI es una matriz que se puede utilizar para comprender cómo viaja la información a través de una red. Este modelo explica de qué manera los paquetes de datos viajan a través de varias capas a otro dispositivo de una red, aun cuando el remitente y el destinatario poseen diferentes tipos de medios de red.

En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red específica.

Fig. 1.5 – Modelo OSI

1.3.2.1.1 Capa Física

Se encarga de pasar bits al medio físico y de suministrar servicios a la siguiente capa. Para ello debe conocer las características mecánicas, eléctricas, funcionales y de procedimiento de las líneas.

1.3.2.1.2 Capa de Enlace de Datos

Esta se encarga de que los datos se envíen con seguridad a su destino y libres de errores. Cuando la conexión no es punto a punto, esta capa no puede asegurar su cometido y es la capa superior quien lo debe hacer .

1.3.2.1.3 Capa de Red

Esta capa se encarga de enlazar con la red y encaminar los datos hacia sus lugares o direcciones de destino. Para esto, se produce un diálogo con la red para establecer prioridades y encaminamientos. Esta y las dos capas inferiores son las encargadas de todo el proceso externo al propio sistema y que están tanto en terminales como en enlaces o repetidores.

1.3.2.1.4 Capa de Transporte

Esta capa se encarga de que los datos enviados y recibidos lleguen en orden, sin duplicar y sin errores. Puede ser servicio de transporte orientado a conexión (conmutación de circuitos o circuitos virtuales) o no orientado a conexión (datagramas).

1.3.2.1.5 Capa de Sesión

Se encarga de proporcionar diálogo entre aplicaciones finales para el uso eficiente de las comunicaciones. Puede agrupar datos de diversas aplicaciones para enviarlos juntos o incluso detener la comunicación y restablecer el envío tras realizar algún tipo de actividad.

1.3.2.1.6 Capa de Presentación

Se encarga de definir los formatos de los datos y si es necesario, procesarlos para su envío. Este proceso puede ser el de compresión o el de paso a algún sistema de codificación. En resumen , se encarga de la sintaxis.

1.3.2.1.7 Capa Aplicación

Esta capa acoge a todas las aplicaciones que requieren la red. Permite que varias aplicaciones compartan la red.

1.3.2.2 Comunicaciones de par a par

Para que los datos puedan viajar desde el origen hasta su destino, cada capa del modelo OSI en el origen debe comunicarse con su capa par en el lugar destino. Esta forma de comunicación se conoce como de par-a-par. Durante este proceso, los protocolos de cada capa intercambian información, denominada unidades de datos de protocolo (PDU). Cada capa de comunicación en el computador origen se comunica con un PDU específico de capa, y con su capa par en el computador destino.

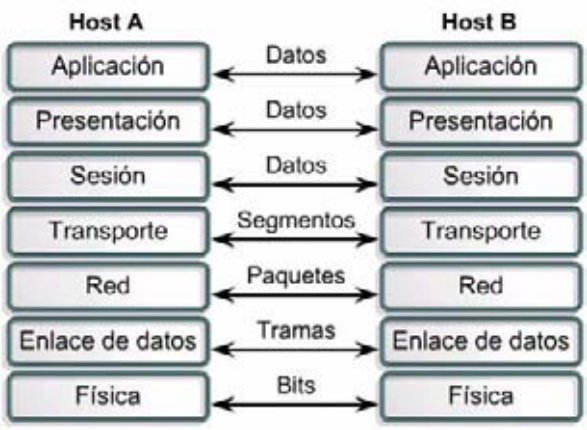

Fig. 1.6 – Comunicaciones de par a par

Los paquetes de datos de una red parten de un origen y se envían a un destino. Cada capa depende de la función de servicio de la capa OSI que se encuentra debajo de ella. Para brindar este servicio, la capa inferior utiliza el encapsulamiento para colocar la PDU de la capa superior en su campo de datos, luego le puede agregar cualquier encabezado e información final que la capa necesite para ejecutar su función. Posteriormente, a medida que los datos se desplazan hacia abajo a través de las capas del modelo OSI, se agregan encabezados e información final adicionales.

1.3.3 Modelo TCP/IP

El estándar histórico y técnico de la Internet es el modelo TCP/IP. El Departamento de Defensa de EE.UU. (DoD) creó el modelo de referencia TCP/IP porque necesitaba diseñar una red que pudiera sobrevivir ante cualquier circunstancia, incluso una guerra nuclear. En un mundo conectado por diferentes tipos de medios de comunicación, como alambres de cobre, microondas, fibras ópticas y enlaces satelitales, el DoD quería que la transmisión de paquetes se realizara cada vez que se iniciaba y bajo cualquier circunstancia. Este difícil problema de diseño dio origen a la creación del modelo TCP/IP.

TCP/IP se desarrolló como un estándar abierto, esto significaba que cualquier persona podía usar el TCP/IP. Esto contribuyó a acelerar el desarrollo de TCP/IP como un estándar. El modelo TCP/IP tiene 4 cuatro capas.

Fig. 1.7 – Modelo TCP/IP

1.3.3.1 Capas del Modelo TCP/IP

Aunque algunas de las capas del modelo TCP/IP tienen el mismo nombre que las capas del modelo OSI, las capas de ambos modelos no se corresponden de manera exacta. cabe destacar que la capa de aplicación posee funciones diferentes en cada modelo.

1.3.3.1.1 Capa de Acceso a la Red

La capa de acceso de red también se denomina capa de host a red. Esta capa es la que maneja todos los aspectos que un paquete IP requiere para efectuar un enlace físico real con los medios de la red. Esta capa incluye los detalles de la tecnología LAN y WAN y todos los detalles de las capas física y de enlace de datos del modelo OSI.

Los controladores para las aplicaciones de software, las tarjetas de módem y otros dispositivos operan en la capa de acceso de red. La capa de acceso de red define los procedimientos para realizar la interfaz con el hardware de la red y para tener acceso al medio de transmisión. Los estándares del protocolo de los módem, tales como el Protocolo Internet de Enlace Serial (SLIP) y el Protocolo de Punto a Punto (PPP) brindan acceso a la red a través de una conexión por módem. Debido a un intrincado juego entre las especificaciones del hardware, el software y los medios de transmisión, existen muchos protocolos que operan en esta capa.

Las funciones de la capa de acceso de red incluyen la asignación de direcciones IP a las direcciones físicas y el encapsulamiento de los paquetes IP en tramas. Basándose en el tipo de

hardware y la interfaz de la red, la capa de acceso de red definirá la conexión con los medios físicos de la misma.

1.3.3.1.2 Capa de Internet

El propósito de la capa de Internet es seleccionar la mejor ruta para enviar paquetes por la red. El protocolo principal que funciona en esta capa es el Protocolo de Internet (IP). La determinación de la mejor ruta y la conmutación de los paquetes ocurre en esta capa.

Los siguientes protocolos operan en la capa de Internet TCP/IP:

- IP proporciona un enrutamiento de paquetes no orientado a conexión de máximo esfuerzo. El IP no se ve afectado por el contenido de los paquetes, sino que busca una ruta de hacia el destino.
- El Protocolo de mensajes de control en Internet (ICMP) suministra capacidades de control y envío de mensajes.
- El Protocolo de resolución de direcciones (ARP) determina la dirección de la capa de enlace de datos, la dirección MAC, para las direcciones IP conocidas.
- El Protocolo de resolución inversa de direcciones (RARP) determina las direcciones IP cuando se conoce la dirección MAC.

El IP ejecuta las siguientes operaciones:

- Define un paquete y un esquema de direccionamiento.
- Transfiere los datos entre la capa Internet y las capas de acceso de red.
- Encamina los paquetes hacia los hosts remotos.

Por último, a veces se considera a IP como protocolo poco confiable. Esto no significa que IP no enviará correctamente los datos a través de la red. Llamar al IP, protocolo poco confiable simplemente significa que IP no realiza la verificación y la corrección de los errores. Dicha función la realizan los protocolos de la capa superior desde las capas de transporte o aplicación.

1.3.3.1.3 Capa de Transporte

La capa de transporte proporciona servicios de transporte desde el host origen hacia el host destino. Esta capa forma una conexión lógica entre los puntos finales de la red, el host transmisor y el host receptor. Los protocolos de transporte segmentan y reensamblan los datos mandados por las capas superiores en el mismo flujo de datos, o conexión lógica entre los extremos. La corriente de datos de la capa de transporte brinda transporte de extremo a extremo.

El control de punta a punta, que se proporciona con las ventanas deslizantes y la confiabilidad de los números de secuencia y acuses de recibo, es el deber básico de la capa de transporte cuando utiliza TCP. La capa de transporte también define la conectividad de extremo a extremo entre las aplicaciones de los hosts. Los servicios de transporte incluyen los siguientes servicios:

TCP y UDP

- Segmentación de los datos de capa superior.
- Envío de los segmentos desde un dispositivo en un extremo a otro dispositivo en otro extremo.

TCP solamente

- Establecimiento de operaciones de punta a punta.
- Control de flujo proporcionado por ventanas deslizantes.
- Confiabilidad proporcionada por los números de secuencia y los acuses de recibo.

Generalmente, se representa la Internet con una nube. La capa de transporte envía los paquetes de datos desde la fuente transmisora hacia el destino receptor a través de la nube. La nube maneja los aspectos tales como la determinación de la mejor ruta.

1.3.3.1.4 Cada de Aplicación

La capa de aplicación del modelo TCP/IP maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y asegura que estos datos estén correctamente empaquetados antes de que pasen a la capa siguiente. TCP/IP incluye no sólo las especificaciones de Internet y de la capa de transporte, tales como IP y TCP, sino también las especificaciones para aplicaciones comunes. TCP/IP tiene protocolos que soportan la transferencia de archivos, e-mail, y conexión remota. Algunos de ellos son los siguientes:

- Protocolo de transferencia de archivos (FTP).
- Protocolo transferencia de hipertexto (HTTP).
- Sistema de archivos de red (NFS).
- Protocolo simple de transferencia de correo (SMTP).
- Emulación de terminal (Telnet).
- Protocolo simple de administración de red (SNMP).
- Sistema de denominación de dominio (DNS).

1.3.4 Comparación de Ambos Modelos

Comparando el modelo OSI con los modelos TCP/IP, surgen algunas similitudes y diferencias.

Las similitudes incluyen:

- Ambos se dividen en capas.
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.
- Ambos tienen capas de transporte y de red similares.
- Ambos modelos deben ser conocidos por los profesionales de networking.
- Ambos suponen que la tecnología es de conmutación por paquetes y no de conmutación por circuito.

Las diferencias incluyen:

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación.
- TCP/IP combina la capa de enlace de datos y la capa física del modelo OSI en la capa de acceso de red.
- TCP/IP parece ser más simple porque tiene menos capas.
- La capa de transporte TCP/IP que utiliza UDP no siempre garantiza la entrega confiable de los paquetes mientras que la capa de transporte del modelo OSI sí.
- Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló la Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, por lo general las redes no se desarrollan a partir del protocolo OSI, aunque el modelo OSI se usa como guía.

Aunque los protocolos TCP/IP representan los estándares en base a los cuales se ha desarrollado la Internet, este currículum utiliza el modelo OSI por los siguientes motivos:

- Es un estándar genérico, independiente de los protocolos.
- Es más detallado, lo que hace que sea más útil para la enseñanza y el aprendizaje.
- Al ser más detallado, resulta de mayor utilidad para el diagnóstico de fallas.
- Los profesionales de networking tienen distintas opiniones con respecto al modelo que se debe usar. Dada la naturaleza de esta industria, es necesario familiarizarse con ambos.

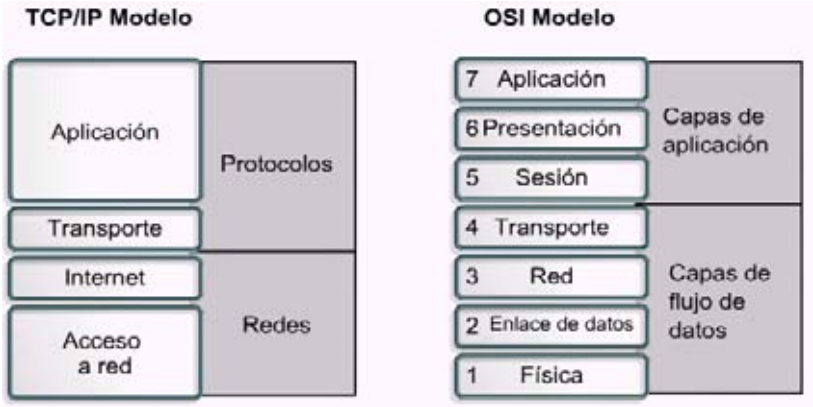

Fig. 1.8 – Comparación entre OSI y TCP/IP

1.4 ETHERNET

La mayor parte del tráfico en Internet se origina y termina en conexiones de Ethernet. Desde su comienzo en la década de 1970, Ethernet ha evolucionado para satisfacer la creciente demanda de LAN de alta velocidad. En el momento en que aparece un nuevo medio, como la fibra óptica, Ethernet se adapta para sacar ventaja de un ancho de banda superior y de un menor índice de errores que la fibra ofrece. Ahora, el mismo protocolo que transportaba datos a 3 Mbps en 1973 transporta datos a 10 Gbps.

El éxito de Ethernet se debe a los siguientes factores:

- Sencillez y facilidad de mantenimiento.
- Capacidad para incorporar nuevas tecnologías.
- Confiabilidad.
- Bajo costo de instalación y de actualización.

Con la llegada de Gigabit Ethernet, lo que comenzó como una tecnología LAN ahora se extiende a distancias que hacen de Ethernet un estándar de Red de Área Metropolitana (MAN) y Red de Área Extensa (WAN).

La idea original de Ethernet nació del problema de permitir que dos o más host utilizaran el mismo medio y evitar que las señales interfirieran entre sí. El problema de acceso por varios usuarios a un medio compartido se estudió a principios de los 70 en la Universidad de Hawai. Se desarrolló un sistema llamado Alohanet para permitir que varias estaciones de las Islas de Hawai tuvieran acceso estructurado a la banda de radiofrecuencia compartida en la atmósfera. Más tarde, este trabajo sentó las bases para el método de acceso a Ethernet conocido como CSMA/CD.

En 1985, el comité de estándares para Redes Metropolitanas y Locales del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) publicó los estándares para las LAN. Estos estándares comienzan con el número 802. El estándar para Ethernet es el 802.3. El IEEE quería asegurar que sus estándares fueran compatibles con el Modelo OSI de la Organización Internacional de Estándares (ISO). Por eso, el estándar IEEE 802.3 debía cubrir las

necesidades de la Capa 1 y de las porciones inferiores de la Capa 2 del modelo OSI. Como resultado, ciertas pequeñas modificaciones al estándar original de Ethernet se efectuaron en el 802.3.

Las diferencias entre los dos estándares fueron tan insignificantes que cualquier tarjeta de interfaz de la red de Ethernet (NIC) puede transmitir y recibir tanto tramas de Ethernet como de 802.3. Básicamente, Ethernet y IEEE 802.3 son un mismo estándar.

Una trama de Ethernet puede partir desde una antigua NIC de 10 Mbps de cable coaxial de un PC, subir a un enlace de fibra de Ethernet de 10 Gbps y terminar en una NIC de 100 Mbps. Siempre que permanezca en redes de Ethernet, el paquete no cambia. Por este motivo, se considera que Ethernet es muy escalable. El ancho de banda de la red podría aumentarse muchas veces sin cambiar la tecnología base de Ethernet.

1.4.1 Ethernet y el Modelo OSI

Ethernet opera en dos áreas del modelo OSI, la mitad inferior de la capa de enlace de datos, conocida como subcapa MAC y la capa física.

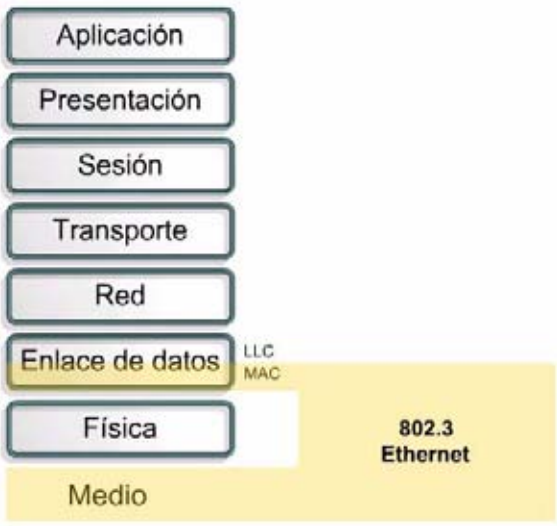

Fig. 1.9 – Ethernet y el Modelo OSI

Para mover datos entre una estación Ethernet y otra, a menudo, estos pasan a través de un repetidor. Todas las demás estaciones del mismo dominio de colisión ven el tráfico que pasa a través del repetidor. Un dominio de colisión es entonces un recurso compartido. Los problemas que se originan en una parte del dominio de colisión generalmente tienen impacto en todo el dominio.

Los estándares garantizan un mínimo ancho de banda y operabilidad especificando el máximo número de estaciones por segmento, la longitud máxima del mismo, el máximo número de repetidores entre estaciones, etc. Las estaciones separadas por repetidores se encuentran dentro del mismo domino de colisión. Las estaciones separadas por puentes o routers se encuentran en dominios de colisión diferentes.

La Figura 1.10 relaciona una variedad de tecnologías Ethernet con la mitad inferior de la Capa 2 y con toda la Capa 1 del modelo OSI. Ethernet en la Capa 1 incluye las interfaces con los medios, señales, corrientes de bits que se transportan en los medios, componentes que transmiten la señal a los medios y las distintas topologías. La Capa 1 de Ethernet tiene un papel clave en la comunicación que se produce entre los dispositivos, pero cada una de estas funciones tiene limitaciones. La Capa 2 se ocupa de estas limitaciones.

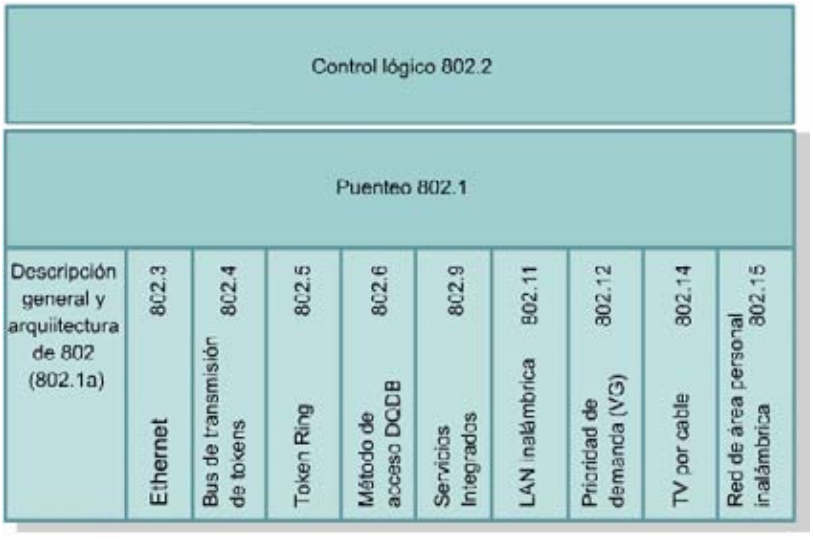

Fig. 1.10 – Estándares IEEE 802.x

Las subcapas de enlace de datos contribuyen significativamente a la compatibilidad de tecnología y comunicación con el computador. La subcapa MAC trata los componentes físicos que se utilizarán para comunicar la información. La subcapa de Control de Enlace Lógico (LLC) sigue siendo relativamente independiente del equipo físico que se utiliza en el proceso de comunicación.

1.4.2 Direccionamiento Físico

Para permitir el envío local de las tramas en Ethernet, se debe contar con un sistema de direccionamiento, una forma de identificar los computadores y las interfaces de manera exclusiva. Ethernet utiliza direcciones MAC que tienen 48 bits de largo y se expresan como doce dígitos hexadecimales. Los primeros seis dígitos hexadecimales, que IEEE administra, identifican al fabricante o al vendedor. Esta porción de la dirección de MAC se conoce como Identificador Exclusivo Organizacional (OUI). Los seis dígitos hexadecimales restantes representan el número de serie de la interfaz u otro valor administrado por el proveedor mismo del equipo. Las direcciones MAC a veces se denominan direcciones grabadas (BIA) ya que estas direcciones se graban en la memoria de sólo lectura (ROM) y se copian en la memoria de acceso aleatorio (RAM) cuando se inicializa la NIC.

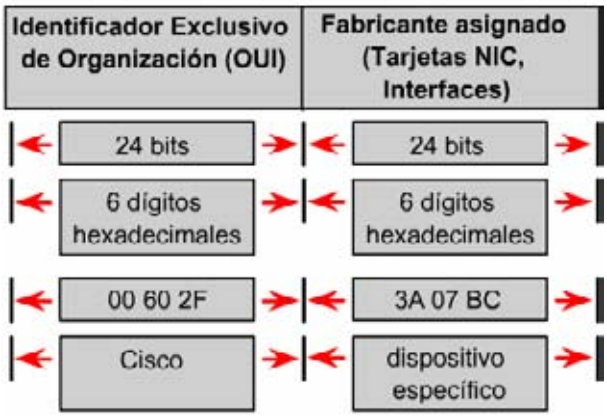

Fig. 1.11 – Formato de la Dirección MAC

La NIC utiliza la dirección MAC para evaluar si el mensaje se debe pasar o no a las capas superiores del modelo OSI. La NIC realiza esta evaluación sin utilizar tiempo de procesamiento de la CPU permitiendo mejores tiempos de comunicación en una red Ethernet.

1.4.3 Estructura de la Trama de Ethernet

En la capa de enlace de datos, la estructura de la trama es casi idéntica para todas las velocidades de Ethernet desde 10 Mbps hasta 10000 Mbps. Sin embargo, en la capa física, casi todas las versiones de Ethernet son sustancialmente diferentes las unas de las otras, teniendo cada velocidad un juego distinto de reglas de diseño arquitectónico.

En la versión de Ethernet desarrollada por DIX antes de la adopción de la versión IEEE 802.3 de Ethernet, el Preámbulo y el Delimitador de Inicio de Trama (SFD) se combinaron en un solo campo, aunque el patrón binario era idéntico. El campo que se denomina Longitud/Tipo aparecía como sólo Longitud en las primeras versiones de IEEE y sólo como Tipo en la versión de DIX. Estos dos usos del campo se combinaron oficialmente en una versión posterior del IEEE, ya que el uso que ambos le daban al campo era común en toda la industria.

El campo Tipo de la Ethernet II se incorporó a la actual definición de trama del 802.3. El nodo receptor debe determinar cuál de los protocolos de capa superior está presente en una trama entrante examinando el campo Longitud/Tipo. Si el valor de los dos octetos es igual o mayor que el de 0x600 (hexadecimal), 1536 (decimal), entonces el contenido del campo de Data es codificado de acuerdo al protocolo indicado

IEEE 802.3						
7	1	6	6	2	64 a 1500	4
Preámbulo	Delimitador de inicio de trama	Direcciónde destino	Dirección origen	Longitud/ Tipo	Encabezado ydatos de 802.2	Secuencia deverificación de trama

Ethernet					
8	6	6	2	64 a 1500	4
Preámbulo	Direcciónde destino	Dirección origen	Tipo	Datos	Secuencia deverificación de trama

Fig. 1.12 – Trama Ethernet

En una red Ethernet, cuando un dispositivo envía datos, puede abrir una ruta de comunicación hacia el otro dispositivo utilizando la dirección MAC destino. El dispositivo origen adjunta un encabezado con la dirección MAC del destino y envía los datos a la red. A medida

que estos datos viajan a través de los medios de red, la NIC de cada dispositivo de la red verifica si su dirección MAC coincide con la dirección destino física que transporta la trama de datos. Si no hay concordancia, la NIC descarta la trama de datos. Cuando los datos llegan al nodo destino, la NIC hace una copia y pasa la trama hacia las capas superiores del modelo OSI. En una red Ethernet, todos los nodos deben examinar el encabezado MAC aunque los nodos que se están comunicando estén lado a lado.

Todos los dispositivos conectados a la LAN de Ethernet tienen interfaces con dirección MAC incluidas las estaciones de trabajo, impresoras, routers y switches.

Algunos de los campos que se permiten o requieren en la trama 802.3 de Ethernet son:

- Preámbulo.
- Delimitador de Inicio de Trama.
- Dirección Destino.
- Dirección Origen.
- Longitud/Tipo.
- Datos y Relleno.
- FCS.
- Extensión.

El *Preámbulo* es un patrón alternado de unos y ceros que se utiliza para la sincronización de los tiempos en implementaciones de 10 Mbps y menores de Ethernet. Las versiones más veloces de Ethernet son síncronas y esta información de temporización es redundante pero se retiene por cuestiones de compatibilidad.

Un *Delimitador de Inicio de Trama* es un campo de un octeto que marca el final de la información de temporización y contiene la secuencia de bits 10101011.

El campo de *Dirección de Destino* contiene la dirección de destino MAC. La dirección de destino puede ser unicast, multicast o de broadcast.

El campo de *Dirección de Origen* contiene la dirección MAC de origen. La dirección de origen generalmente es la dirección unicast del nodo de transmisión de Ethernet. Sin embargo, existe un número creciente de protocolos virtuales en uso que utilizan y a veces comparten una dirección MAC origen específica para identificar la entidad virtual.

El campo *Longitud/Tipo* admite dos usos diferentes. Si el valor es menor a 1536 decimal, 0x600 (hexadecimal), entonces el valor indica la longitud. La interpretación de la longitud se utiliza cuando la Capa LLC proporciona la identificación del protocolo. El valor del tipo especifica el protocolo de capa superior que recibe los datos una vez que se ha completado el procesamiento de Ethernet. La longitud indica la cantidad de bytes de datos que sigue este campo.

Los campos de *Datos y Relleno*, de ser necesario, pueden tener cualquier longitud, mientras que la trama no exceda el tamaño máximo permitido de trama. La unidad máxima de transmisión (MTU) para Ethernet es de 1500 octetos, de modo que los datos no deben superar dicho tamaño. El contenido de este campo no está especificado. Se inserta un relleno no especificado inmediatamente después de los datos del usuario cuando no hay suficientes datos de usuario para que la trama cumpla con la longitud mínima especificada. Ethernet requiere que cada trama tenga entre 64 y 1518 octetos de longitud.

Una *FCS* contiene un valor de verificación CRC de 4 bytes, creado por el dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas. Ya que la corrupción de un solo bit en cualquier punto desde el inicio de la dirección destino hasta el extremo del campo de FCS hará que la checksum (suma de verificación) sea diferente, la cobertura de la FCS se auto-incluye. No es posible distinguir la corrupción de la FCS en sí y la corrupción de cualquier campo previo que se utilizó en el cálculo.

1.4.4 CSMA/CD

Ethernet es una tecnología de broadcast de medios compartidos. El método de acceso CSMA/CD que se usa en Ethernet ejecuta tres funciones:

- Transmitir y recibir paquetes de datos.

- Decodificar paquetes de datos y verificar que las direcciones sean válidas antes de transferirlos a las capas superiores del modelo OSI.
- Detectar errores dentro de los paquetes de datos o en la red.

En el método de acceso CSMA/CD, los dispositivos de networking que tienen datos para transmitir funcionan en el modo "escuchar antes de transmitir". Esto significa que cuando un nodo desea enviar datos, primero debe determinar si los medios de networking están ocupados. Si el nodo determina que la red está ocupada, el nodo esperará un tiempo determinado al azar antes de reintentar. Si el nodo determina que el medio de networking no está ocupado, comenzará a transmitir y a escuchar. El nodo escucha para asegurarse que ninguna otra estación transmita al mismo tiempo. Una vez que ha terminado de transmitir los datos, el dispositivo vuelve al modo de escuchar.

Los dispositivos de networking detectan que se ha producido una colisión cuando aumenta la amplitud de la señal en los medios de networking.

Cuando se produce una colisión, cada nodo que se encuentra en transmisión continúa transmitiendo por poco tiempo a fin de asegurar que todos los dispositivos detecten la colisión. Una vez que todos los dispositivos la han detectado, se invoca el algoritmo de postergación y la transmisión se interrumpe. Los nodos interrumpen la transmisión por un período determinado al azar, que es diferente para cada dispositivo. Cuando caduca el período de retardo cada nodo puede intentar ganar acceso al medio de networking. Los dispositivos involucrados en la colisión no tienen prioridad para transmitir datos.

1.4.5 Tecnologías Ethernet

Ethernet ha sido la tecnología LAN de mayor éxito, en gran medida, debido a la simplicidad de su implementación, cuando se la compara con otras tecnologías. Ethernet también ha tenido éxito porque es una tecnología flexible que ha evolucionado para satisfacer las cambiantes necesidades y capacidades de los medios.

Las modificaciones a Ethernet han resultado en significativos adelantos, desde la tecnología a 10 Mbps usada a principios de principios de los 80. El estándar de Ethernet de 10

Mbps no sufrió casi ningún cambio hasta 1995 cuando el IEEE anunció un estándar para Fast Ethernet de 100 Mbps. En los últimos años, un crecimiento aún más rápido en la velocidad de los medios ha generado la transición de Fast Ethernet (Ethernet Rápida) a Gigabit Ethernet (Ethernet de 1 Gigabit). Inclusive, una versión de Ethernet aún más rápida, Ethernet de 10 Gigabits (10 Gigabit Ethernet) se halla fácilmente en el mercado.

En estas versiones más rápidas de Ethernet, el direccionamiento MAC, CSMA/CD y el formato de trama no han sufrido cambios respecto de versiones anteriores de Ethernet. Sin embargo, otros aspectos de la subcapa MAC, la capa física y el medio han cambiado. Las tarjetas de interfaz de red (NIC) con base de cobre capaces de operar a 10/100/1000 están ahora entre las más comunes. Los switches y los routers con puertos de Gigabit se están convirtiendo en el estándar para los armarios de cableado. El uso de la fibra óptica que admite Gigabit Ethernet se considera un estándar para el cableado backbone en la mayoría de las instalaciones nuevas.

Fig. 1.13 – Tipos de Ethernet

1.4.6 Ethernet de 1000 Mbps

Los estándares para Ethernet de 1000 Mbps o Gigabit Ethernet representan la transmisión a través de medios ópticos y de cobre. El estándar para 1000BASE-X, IEEE 802.3z, especifica una conexión full duplex de 1 Gbps en fibra óptica. El estándar para 1000BASE-T, IEEE 802.3ab, especifica el uso de cable de cobre balanceado de Categoría 5, o mejor.

Las 1000BASE-TX, 1000BASE-SX y 1000BASE-LX utilizan los mismos parámetros de temporización. Utilizan un tiempo de bit de 1 nanosegundo. La trama de Gigabit Ethernet presenta el mismo formato que se utiliza en Ethernet de 10 y 100-Mbps. Según su implementación, Gigabit Ethernet puede hacer uso de distintos procesos para convertir las tramas a bits en el cable. (Fig. 1.12)

Las diferencias entre Ethernet estándar, Fast Ethernet y Gigabit Ethernet se encuentran en la capa física. Debido a las mayores velocidades de estos estándares recientes, la menor duración de los tiempos de bit requiere una consideración especial. Como los bits ingresan al medio por menor tiempo y con mayor frecuencia, es fundamental la temporización. Esta transmisión a alta velocidad requiere de frecuencias cercanas a las limitaciones de ancho de banda para los medios de cobre. Esto hace que los bits sean más susceptibles al ruido en los medios de cobre.

Estos problemas requieren que Gigabit Ethernet utilice dos distintos pasos de codificación. La transmisión de datos se realiza de manera más eficiente utilizando códigos para representar la corriente binaria de bits. Los datos codificados proporcionan sincronización, uso eficiente del ancho de banda y mejores características de la Relación entre Señal y Ruido.

En la capa física, los patrones de bits a partir de la capa MAC se convierten en símbolos. Los símbolos también pueden ser información de control tal como trama de inicio, trama de fin, condiciones de inactividad del medio. La trama se codifica en símbolos de control y símbolos de datos para aumentar la tasa de transferencia de la red.

Gigabit Ethernet (1000BASE-X) con base de fibra utiliza una codificación 8B/10B que es similar a la del concepto 4B/5B. Entonces, le sigue la simple codificación de línea Sin Retorno a Cero (NRZ) de la luz en la fibra óptica. Este proceso de codificación más sencillo es posible debido a que el medio de la fibra puede transportar señales de mayor ancho de banda

1.4.6.1 1000BASE-T

1000BASE-T (IEEE 802.3ab), se desarrolló para proporcionar ancho de banda adicional a fin de ayudar a aliviar cuellos de botella producidos en 100BASE-T. Proporciona un mayor desempeño a dispositivos, tales como backbones dentro de los edificios, enlaces entre los switches, servidores centrales y otras aplicaciones de armarios para cableado, así como conexiones para estaciones de trabajo de nivel superior. Fast Ethernet se diseñó para funcionar en los cables de cobre Cat 5 existentes y esto requirió que dicho cable aprobara la verificación de la Cat 5e. La mayoría de los cables Cat 5 instalados pueden aprobar la certificación 5e si están correctamente terminados. Uno de los atributos más importantes del estándar para 1000BASE-T es que es interoperable con 10BASE-T y 100BASE-TX.

Como el cable Cat 5e puede transportar, de forma confiable, hasta 125 Mbps de tráfico, obtener 1000 Mbps (Gigabit) de ancho de banda fue un desafío de diseño. El primer paso para lograr una 1000BASE-T es utilizar los cuatro pares de hilos en lugar de los dos pares tradicionales utilizados para 10BASE-T y 100BASE-TX. Esto se logra mediante un sistema de circuitos complejo que permite las transmisiones full duplex en el mismo par de hilos. Esto proporciona 250 Mbps por par. Con los cuatro pares de hilos, proporciona los 1000 Mbps esperados. Como la información viaja simultáneamente a través de las cuatro rutas, el sistema de circuitos tiene que dividir las tramas en el transmisor y reensamblarlas en el receptor.

La codificación de 1000BASE-T con la codificación de línea 4D-PAM5 se utiliza en UTP de Cat 5e o superior. Esto significa que la transmisión y recepción de los datos se produce en ambas direcciones en el mismo hilo a la vez. Como es de esperar, esto provoca una colisión permanente en los pares de hilos. Estas colisiones generan patrones de voltaje complejos. Mediante los complejos circuitos integrados que usan técnicas, tales como la cancelación de eco, la Corrección del Error de Envío Capa 1 (FEC) y una prudente selección de los niveles de voltaje, el sistema logra una tasa de transferencia de 1 Gigabit.

En los períodos de inactividad, son nueve los niveles de voltaje que se encuentran en el cable y durante los períodos de transmisión de datos son 17. Con este gran número de estados y con los efectos del ruido, la señal en el cable parece más analógica que digital. Como en el

caso del analógico, el sistema es más susceptible al ruido debido a los problemas de cable y terminación.

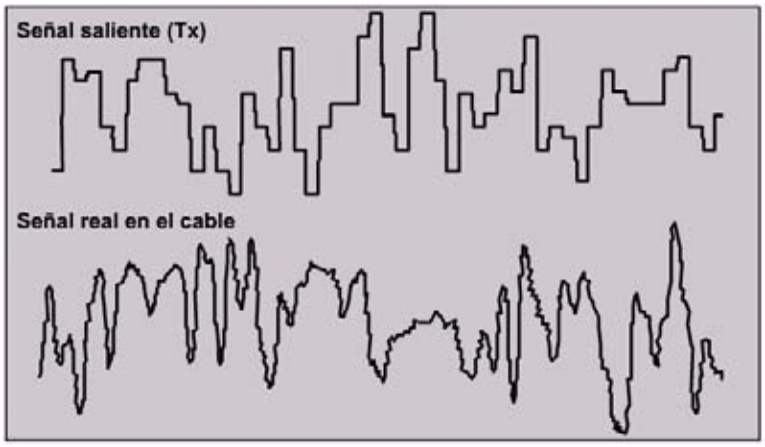

Fig. 1.14 – Señal de TX 1000BASE-T

Los datos que provienen de la estación transmisora se dividen cuidadosamente en cuatro corrientes paralelas; luego se codifican, se transmiten y se detectan en paralelo y finalmente se reensamblan en una sola corriente de bits recibida. 1000BASE-T admite tanto las operaciones en half-duplex como las en full-duplex. El uso de 1000BASE-T en full-duplex está ampliamente difundido.

1.4.6.2 1000BASE-SX y LX

El estándar IEEE 802.3 recomienda Gigabit Ethernet en fibra como la tecnología de backbone de preferencia.

La temporización, el formato de trama y la transmisión son comunes a todas las versiones de 1000 Mbps. En la capa física, se definen dos esquemas de codificación de la señal. El esquema 8B/10B se utiliza para los medios de fibra óptica y de cobre blindado y la modulación de amplitud de pulso 5 (PAM5) se utiliza para los UTP.

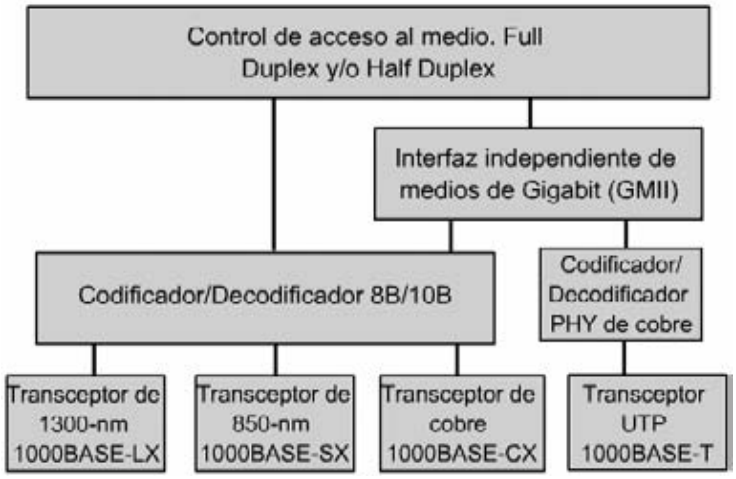

Fig. 1.15 – Capas de Gigabit Ethernet

1000BASE-X utiliza una codificación 8B/10B convertida en la codificación de línea sin retorno a cero (NRZ). La codificación NRZ depende del nivel de la señal encontrado en la ventana de temporización para determinar el valor binario para ese período de bits. A diferencia de la mayoría de los otros esquemas de codificación descritos, este sistema de codificación va dirigido por los niveles en lugar de por los bordes. Es decir, determinar si un bit es un cero o un uno depende del nivel de la señal en vez del momento cuando la señal cambia de nivel.

Las señales NRZ son entonces pulsadas hacia la fibra utilizando fuentes de luz de onda corta o de onda larga. La onda corta utiliza un láser de 850 nm o una fuente LED en fibra óptica multimodo (1000BASE-SX). Es la más económica de las opciones pero cubre distancias más cortas. La fuente láser de 1310 nm de onda larga utiliza fibra óptica monomodo o multimodo (1000BASE-LX). Las fuentes de láser utilizadas con fibra monomodo pueden cubrir distancias de hasta 5000 metros. Debido al tiempo necesario para encender y apagar por completo el LED o el láser cada vez, la luz se pulsa utilizando alta y baja energía. La baja energía representa un cero lógico y la alta energía, un uno lógico.

El método de Control de Acceso a los Medios considera el enlace como si fuera de punto a punto. Como se utilizan distintas fibras para transmitir (TX) y recibir (RX) la conexión de por sí es de full duplex. Gigabit Ethernet permite un sólo repetidor entre dos estaciones.

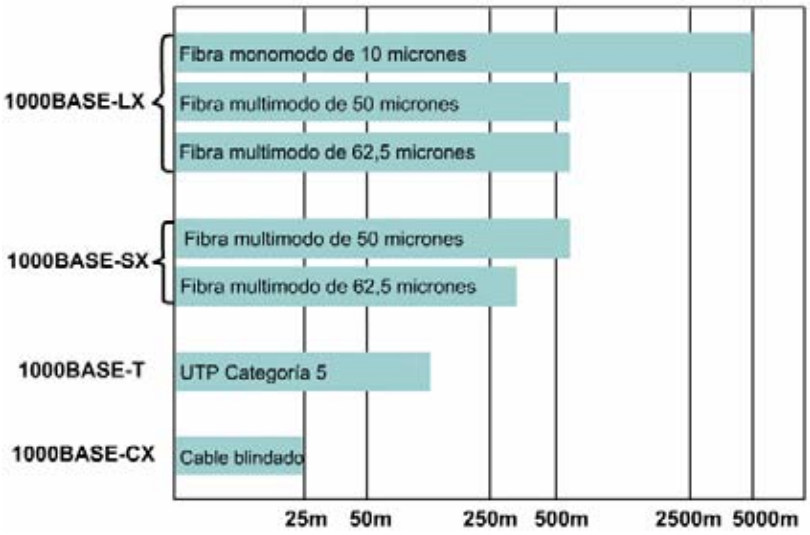

Fig. 1.16 – Comparación de medios de Gigabit Ethernet

1.4.6.3 Arquitectura de 1000 Mbps

Las limitaciones de distancia de los enlaces full-duplex están restringidas sólo por el medio y no por el retardo de ida y vuelta. Como la mayor parte de Gigabit Ethernet está conmutada, los valores de las Figuras 1.18 y 1.19 son los límites prácticos entre los dispositivos. Las topologías de cadena de margaritas, de estrella y de estrella extendida están todas permitidas. El problema entonces yace en la topología lógica y el flujo de datos y no en las limitaciones de temporización o distancia.

Medio	Ancho de banda modal	Distancia máxima
Fibra multimodo 62,5µm	160	220 m
Fibra multimodo 62,5µm	200	275 m
Fibra multimodo 50µm	400	500 m
Fibra multimodo 50µm	500	500 m

Fig. 1.17 – Distancias de cable máximas 1000BASE-SX

Medio	Ancho de banda modal	Distancia máxima
Fibra multimodo 62,5µm	500	550 m
Fibra multimodo 50µm	400	550 m
Fibra multimodo 50µm	500	550 m
Fibra multimodo 10µm	N/A	5000 m

Fig. 1.18 – Distancias de cable máximas 1000BASE-LX

Un cable UTP de 1000BASE-T es igual que un cable de una 10BASE-T o 100BASE-TX, excepto que el rendimiento del enlace debe cumplir con los requisitos de mayor calidad de ISO Clase D (2000) o de la Categoría 5e.

No es recomendable modificar las reglas de arquitectura de 1000BASE-T. A los 100 metros, 1000BASE-T opera cerca del límite de la capacidad de su hardware para recuperar la señal transmitida. Cualquier problema de cableado o de ruido ambiental podría dejar un cable, que en los demás aspectos cumple con los estándares, inoperable inclusive a distancias que se encuentran dentro de la especificación.

Se recomienda que todos los enlaces existentes entre una estación y un hub o switch estén configurados para Auto-Negociación para así permitir el mayor rendimiento conjunto. Esto evitará errores accidentales en la configuración de otros parámetros necesarios para una adecuada operación de Gigabit Ethernet.

1.4.6.4 10 Gigabit Ethernet

Se adaptó el IEEE 802.3ae para incluir la transmisión en full-duplex de 10 Gbps en cable de fibra óptica. Las similitudes básicas entre 802.3ae y 802.3, Ethernet original son notables. Ethernet de 10-Gigabit (10GbE) está evolucionando no sólo para las LAN sino también para las MAN y las WAN.

Con un formato de trama y otras especificaciones de Capa 2 de Ethernet compatibles con estándares anteriores, 10GbE puede proporcionar mayores necesidades de ancho de banda que son interoperables con la infraestructura de red existente.

Un importante cambio conceptual en Ethernet surge con 10GbE. Por tradición, se considera que Ethernet es una tecnología de LAN, pero los estándares de la capa física de 10GbE permiten tanto una extensión de las distancias de hasta 40 km a través de una fibra monomodo como una compatibilidad con la red óptica síncrona (SONET) y con redes síncronas de jerarquía digital (SDH). La operación a una distancia de 40 km hace de 10GbE una tecnología MAN viable. La compatibilidad con las redes SONET/SDH que operan a velocidades

de hasta OC-192 (9.584640 Gbps) hace de 10GbE una tecnología WAN viable. Es posible que 10GbE compita con ATM en ciertas aplicaciones

1.4.7 El Futuro de Ethernet

Ethernet ha evolucionado desde las primeras tecnologías, a las Tecnologías Fast, a las de Gigabit y a las de MultiGigabit. Aunque otras tecnologías LAN todavía están instaladas (instalaciones antiguas), Ethernet domina las nuevas instalaciones de LAN. A tal punto que algunos llaman a Ethernet el "tono de marcación" de la LAN. Ethernet ha llegado a ser el estándar para las conexiones horizontales, verticales y entre edificios. Las versiones de Ethernet actualmente en desarrollo están borrando la diferencia entre las redes LAN, MAN y WAN.

Mientras que Ethernet de 1 Gigabit es muy fácil de hallar en el mercado, y cada vez es más fácil conseguir los productos de 10 Gigabits, el IEEE y la Alianza de Ethernet de 10 Gigabits se encuentran trabajando en estándares para 40, 100 e inclusive 160 Gbps. Las tecnologías que se adopten dependerán de un número de factores que incluyen la velocidad de maduración de las tecnologías y de los estándares, la velocidad de adopción por parte del mercado y el costo.

Se han presentando propuestas para esquemas de arbitraje de Ethernet, que no sean CSMA/CD. El problema de las colisiones con las topologías físicas en bus de 10BASE5 y 10BASE2 y de los hubs de 10BASE-T y 100BASE-TX ya no es tan frecuente. El uso de UTP y de la fibra óptica con distintas rutas de TX y RX y los costos reducidos de los switches hacen que las conexiones a los medios en half-duplex y los medios únicos compartidos sean mucho menos importantes.

El futuro de los medios para networking tiene tres ramas:

- Cobre (hasta 1000 Mbps, tal vez más)
- Inalámbrico (se aproxima a los 100 Mbps, tal vez más)
- Fibra óptica (en la actualidad a una velocidad de 10.000 Mbps y pronto superior)

Los medios de cobre e inalámbricos presentan ciertas limitaciones físicas y prácticas en cuanto a la frecuencia más alta con la se pueda transmitir una señal. Este no es un factor limitante para la fibra óptica en un futuro predecible. Las limitaciones de ancho de banda en la fibra óptica son extremadamente amplias y todavía no están amenazadas. En los sistemas de fibra, son la tecnología electrónica (por ejemplo los emisores y los detectores) y los procesos de fabricación de la fibra los que más limitan la velocidad. Los adelantos futuros de Ethernet probablemente estén dirigidos hacia las fuentes de luz láser y a la fibra óptica monomodo.
Cuando Ethernet era más lenta, en half-duplex, sujeta a colisiones y a un proceso "democrático" de prioridades, no se consideraba que tuviera las capacidades de Calidad de Servicio (QoS) necesarias para manejar cierto tipo de tráfico. Esto incluía por ejemplo la telefonía IP y el video multicast.

Las tecnologías de Ethernet de alta velocidad y full-duplex que ahora dominan el mercado están resultando ser suficientes a la hora de admitir aplicaciones intensivas inclusive las de QoS. Esto hace que las potenciales aplicaciones de Ethernet sean aún más amplias. Irónicamente, la capacidad de QoS de punta a punta ayudó a dar un empuje a ATM para escritorio y a la WAN a mediados de los 90, pero ahora es Ethernet y no ATM la que está realizando este objetivo

1.5 CONMUTACIÓN DE ETHERNET

Ethernet compartida funciona muy bien en circunstancias ideales. Cuando el número de dispositivos que intentan acceder a la red es bajo, el número de colisiones permanece dentro de los límites aceptables. Sin embargo, cuando el número de usuarios de la red aumenta, el mayor número de colisiones puede causar que el rendimiento sea intolerablemente malo. El puenteo se desarrolló para aliviar los problemas de rendimiento que surgieron con el aumento de las colisiones. La conmutación surgió del puenteo y se ha convertido en la tecnología clave de las LAN modernas de Ethernet.

Las colisiones y broadcasts son sucesos esperados en la networking moderna. Ellas, de hecho, están planeadas dentro del diseño de Ethernet y de las tecnologías de capa avanzadas. Sin embargo, cuando las colisiones y broadcasts ocurren en un número que se encuentra por encima del óptimo, el rendimiento de la red se ve afectado. El concepto de dominios de colisión

y de broadcast trata las formas en que pueden diseñarse las redes para limitar los efectos negativos de las colisiones y broadcasts.

1.5.1 Conmutación a Nivel de Capa 2

A medida que se agregan más nodos al segmento físico de Ethernet, aumenta la contención de los medios. Ethernet es un medio compartido, lo que significa que sólo un nodo puede transmitir datos a la vez. Al agregar más nodos, se aumenta la demanda sobre el ancho de banda disponible y se impone una carga adicional sobre los medios. Cuando aumenta el número de nodos en un solo segmento, aumenta la probabilidad de que haya colisiones, y esto causa más retransmisiones. Una solución al problema es dividir un segmento grande en partes y separarlo en dominios de colisión aislados. Para lograr esto, un puente guarda una tabla de direcciones MAC y sus puertos asociados. El puente luego envía o descarta tramas basándose en las entradas de su tabla.

Un puente sólo tiene dos puertos y divide un dominio de colisión en dos partes. Todas las decisiones que toma el puente se basan en un direccionamiento MAC o de Capa 2 y no afectan el direccionamiento lógico o de Capa 3. Así, un puente dividirá el dominio de colisión pero no tiene efecto sobre el dominio lógico o de broadcast. No importa cuántos puentes haya en la red, a menos que haya un dispositivo como por ejemplo un router que funciona en el direccionamiento de Capa 3, toda la red compartirá el mismo espacio de dirección lógica de broadcast. Un puente creará más dominios de colisión pero no agregará dominios de broadcast.

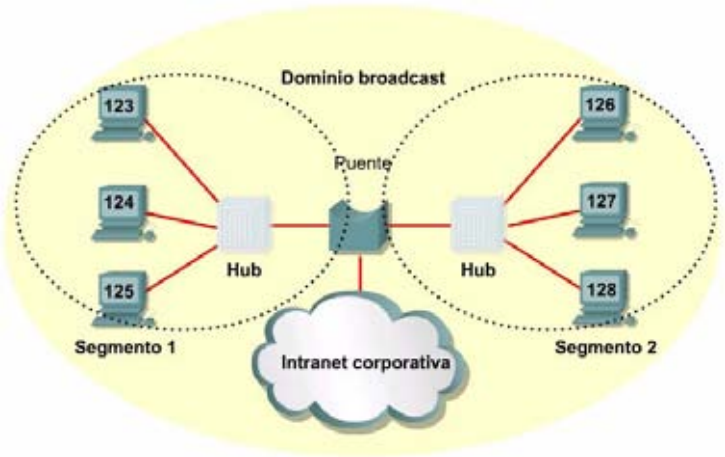

Fig. 1.19 – Puentes

1.5.2 Operación de Switches

Un switch es simplemente un puente multipuerto. Cuando sólo un nodo está conectado a un puerto de switch, el dominio de colisión en el medio compartido contiene sólo dos nodos. Los dos nodos en este pequeño segmento, o dominio de colisión, constan del puerto de switch y el host conectado a él. Estos segmentos físicos pequeños son llamados microsegmentos. Otra capacidad emerge cuando sólo dos nodos se conectan. En una red que utiliza cableado de par trenzado, un par se usa para llevar la señal transmitida de un nodo al otro. Un par diferente se usa para la señal de retorno o recibida. Es posible que las señales pasen a través de ambos pares de forma simultánea. La capacidad de comunicación en ambas direcciones al mismo tiempo se conoce como full duplex. La mayoría de los switch son capaces de admitir full duplex, como también lo son las tarjetas de interfaz de red. En el modo full duplex, no existe contención para los medios. Así, un dominio de colisión ya no existe. En teoría, el ancho de banda se duplica cuando se usa full duplex.

Además de la aparición de microprocesadores y memoria más rápidos, otros dos avances tecnológicos hicieron posible la aparición de los switch. La memoria de contenido direccionable (Content Addressable Memory, CAM) es una memoria que esencialmente funciona al revés en comparación con la memoria convencional. Ingresar datos a la memoria devolverá la dirección asociada. El uso de memoria CAM permite que un switch encuentre directamente el puerto que está asociado con la dirección MAC sin usar un algoritmo de búsqueda. Un circuito integrado de aplicación específica (Application Specific Integrated Circuit, ASIC) es un dispositivo formado de compuertas lógicas no dedicadas que pueden programarse para realizar funciones a velocidades lógicas. Las operaciones que antes se llevaban a cabo en software ahora pueden hacerse en hardware usando ASIC. El uso de estas tecnologías redujo enormemente los retardos causados por el procesamiento del software y permitió que un switch pueda mantenerse al ritmo de la demanda de los datos de muchos microsegmentos y velocidades de bits altas

1.5.3 Latencia

La latencia es el retardo que se produce entre el tiempo en que una trama comienza a dejar el dispositivo origen y el tiempo en que la primera parte de la trama llega a su destino.

Existe una gran variedad de condiciones que pueden causar retardos mientras la trama viaja desde su origen a su destino:

- Retardos de los medios causados por la velocidad limitada a la que las señales pueden viajar por los medios físicos.
- Retardos de circuito causados por los sistemas electrónicos que procesan la señal a lo largo de la ruta.
- Retardos de software causados por las decisiones que el software debe tomar para implementar la conmutación y los protocolos.
- Retardos causados por el contenido de la trama y en qué parte de la trama se pueden tomar las decisiones de conmutación. Por ejemplo, un dispositivo no puede enrutar una trama a su destino hasta que la dirección MAC destino haya sido leída.

1.5.4 Modos de Conmutación

Cómo se conmuta una trama a su puerto de destino es una compensación entre la latencia y la confiabilidad. Un switch puede comenzar a transferir la trama tan pronto como recibe la dirección MAC destino. La conmutación en este punto se llama conmutación por el método de corte y da como resultado una latencia más baja en el switch. Sin embargo, no se puede verificar la existencia de errores. En el otro extremo, el switch puede recibir toda la trama antes de enviarla al puerto destino. Esto le da al software del switch la posibilidad de controlar la secuencia de verificación de trama (Frame Check Sequence, FCS) para asegurar que la trama se haya recibido de modo confiable antes de enviarla al destino. Si se descubre que la trama es inválida, se descarta en este switch en vez de hacerlo en el destino final. Ya que toda la trama se almacena antes de ser enviada, este modo se llama de almacenamiento y envío. El punto medio entre los modos de corte y de almacenamiento y envío es el modo libre de fragmentos. El modo libre de fragmentos lee los primeros 64 bytes, que incluye el encabezado de la trama, y la conmutación comienza antes de que se lea todo el campo de datos y la checksum. Este modo verifica la confiabilidad de direccionamiento y la información del protocolo de control de enlace lógico (Logical Link Control, LLC) para asegurar que el destino y manejo de los datos sean correctos.

Al usar conmutación por métodos de corte, tanto el puerto origen como el destino deben operar a la misma velocidad de bit para mantener intacta la trama. Esto se denomina conmutación síncrona. Si las velocidades de bit no son iguales, la trama debe almacenarse a una velocidad de bit determinada antes de ser enviada a otra velocidad de bit. Esto se conoce como conmutación asíncrona. En la conmutación asimétrica se debe usar el método de almacenamiento y envío.

Una conmutación asimétrica proporciona conexiones conmutadas entre puertos con distinto ancho de banda, tal como una combinación de puertos de 1000 Mbps y de 100 Mbps. La conmutación asimétrica ha sido optimizada para el flujo de tráfico cliente/servidor en el que muchos clientes se comunican con el servidor de forma simultánea, lo cual requiere mayor ancho de banda dedicado al puerto del servidor para evitar un cuello de botella en ese puerto.

1.5.5 Dominios de Colisión

Los dominios de colisión son los segmentos de red física conectados, donde pueden ocurrir colisiones. Las colisiones causan que la red sea ineficiente. Cada vez que ocurre una colisión en la red, se detienen todas las transmisiones por un período de tiempo. La duración de este período sin transmisión varía y depende de un algoritmo de postergación para cada dispositivo de la red.

1.5.6 Segmentación

Conectar varios computadores a un solo medio de acceso compartido que no tiene ningún otro dispositivo de networking conectado, crea un dominio de colisión. Esta situación limita el número de computadores que pueden utilizar el medio, también llamado segmento. Los dispositivos de Capa 1 amplían pero no controlan los dominios de colisión.

Los dispositivos de Capa 2 dividen o segmentan los dominios de colisión. El control de propagación de trama con la dirección MAC asignada a todos los dispositivos de Ethernet ejecuta esta función. Los dispositivos de Capa 2 hacen un seguimiento de las direcciones MAC y el segmento en el que se encuentran. Al hacer esto, estos dispositivos pueden controlar el flujo de tráfico en el nivel de Capa 2 haciendo que las redes sean más eficientes, al permitir que

los datos se transmitan por diferentes segmentos de la LAN al mismo tiempo sin que las tramas colisionen. Al usar puentes y switches, el dominio de colisión se divide efectivamente en partes más pequeñas, que se transforman cada una a su vez en un dominio de colisión.

Estos dominios de colisión más pequeños tendrán menos hosts y menos tráfico que el dominio original. Los dispositivos de Capa 3, al igual que los de Capa 2, no envían las colisiones. Es por eso que usar dispositivos de Capa 3 en una red produce el efecto de dividir los dominios de colisión en dominios menores.

1.5.7 Broadcasts de Capa 2

Para comunicarse con todos los dominios de colisión, los protocolos utilizan tramas de broadcast y multicast a nivel de Capa 2 en el modelo OSI. Cuando un nodo necesita comunicarse con todos los hosts de la red, envía una trama de broadcast con una dirección MAC destino 0xFFFFFFFFFFFF. Esta es una dirección a la cual debe responder la tarjeta de interfaz de la red de cada host.

Los dispositivos de Capa 2 deben inundar todo el tráfico de broadcast y multicast. La acumulación de tráfico de broadcast y multicast de cada dispositivo de la red se denomina radiación de broadcast. En algunos casos, la circulación de radiación de broadcast puede saturar la red, entonces no hay ancho de banda disponible para los datos de las aplicaciones. En este caso, no se pueden establecer las conexiones en la red, y las conexiones existentes pueden descartarse, algo que se conoce como tormenta de broadcast. La probabilidad de las tormentas de broadcast aumenta a medida que crece la red conmutada.

Como la NIC tiene que interrumpir a la CPU para procesar cada grupo de broadcast o multicast al que pertenece, el efecto de radiación de broadcast afecta el rendimiento de los hosts de la red. La mayoría de las veces, el host no se beneficia al procesar el broadcast, ya que no es el destino buscado. Al host no le interesa el servicio que se publicita, o ya lo conoce. Los niveles elevados de radiación de broadcast pueden degradar el rendimiento del host de manera considerable. Las tres fuentes de broadcasts y multicasts en las redes IP son las estaciones de trabajo, los routers y las aplicaciones multicast.

Las estaciones de trabajo envían en broadcast una petición de protocolo de resolución de direcciones (Address Resolution Protocol, ARP) cada vez que necesitan ubicar una dirección MAC que no se encuentra en la tabla ARP.

Los protocolos de enrutamiento que están configurados en la red pueden aumentar el tráfico de broadcast de modo significativo. Algunos administradores configuran todas las estaciones de trabajo para que ejecuten el protocolo de información de enrutamiento (Routing Information Protocol, RIP) como una política de redundancia y alcance. Cada 30 segundos, el RIPv1 utiliza broadcasts para retransmitir toda la tabla de enrutamiento a otros routers RIP.

Las aplicaciones multicast en IP pueden afectar negativamente el rendimiento de redes conmutadas de gran escala. Aunque el multicast es una forma eficiente de enviar un flujo de datos de multimedia a muchos usuarios en un hub de medios compartidos, afecta a cada usuario de una red plana conmutada. Una aplicación de paquete de video determinada, puede generar un flujo de siete megabytes de datos multicast que, en una red conmutada, se enviarían a cada segmento, causando una gran congestión.

1.5.8 Dominios de Broadcast

Un dominio de broadcast es un grupo de dominios de colisión conectados por dos dispositivos de Capa 2. Dividir una LAN en varios dominios de colisión aumenta la posibilidad de que cada host de la red tenga acceso a los medios. Efectivamente, esto reduce la posibilidad de colisiones y aumenta el ancho de banda disponible para cada host. Pero los dispositivos de Capa 2 envían broadcasts, y si son excesivos, pueden reducir la eficiencia de toda la LAN. Los broadcasts deben controlarse en la Capa 3, ya que los dispositivos de Capa 1 y Capa 2 no pueden hacerlo. El tamaño total del dominio del broadcast puede identificarse al observar todos los dominios de colisión que procesan la misma trama de broadcast. En otras palabras, todos los nodos que forman parte de ese segmento de red delimitados por un dispositivo de Capa 3. Los dominios de broadcast están controlados en la Capa 3 porque los routers no envían broadcasts. Los routers, en realidad, funcionan en las Capas 1, 2 y 3. Ellos, al igual que los dispositivos de Capa 1, poseen una conexión física y transmiten datos a los medios. Ellos tienen un encapsulamiento de Capa 2 en todas las interfaces y se comportan como cualquier

otro dispositivo de Capa 2. Es la Capa 3 la que permite que el router segmente dominios de broadcast.

Para que un paquete sea enviado a través del router, el dispositivo de Capa 2 debe ya haberlo procesado y la información de la trama debe haber sido eliminada. El envío de Capa 3 se basa en la dirección IP destino y no en la dirección MAC. Para que un paquete pueda enviarse, debe contener una dirección IP que esté por afuera del alcance de las direcciones asignadas a la LAN, y el router debe tener un destino al cual enviar el paquete específico en su tabla de enrutamiento.

1.6 LAN VIRTUALES

1.6.1 Introducción a las VLAN

Una VLAN es una agrupación lógica de estaciones, servicios y dispositivos de red que no se limita a un segmento de LAN físico.

Las VLAN facilitan la administración de grupos lógicos de estaciones y servidores que se pueden comunicar como si estuviesen en el mismo segmento físico de LAN. También facilitan la administración de mudanzas, adiciones y cambios en los miembros de esos grupos.

Las VLAN segmentan de manera lógica las redes conmutadas según las funciones laborales, departamentos o equipos de proyectos, sin importar la ubicación física de los usuarios o las conexiones físicas a la red. Todas las estaciones de trabajo y servidores utilizados por un grupo de trabajo en particular comparten la misma VLAN, sin importar la conexión física o la ubicación.

La configuración o reconfiguración de las VLAN se logra mediante el software. Por lo tanto, la configuración de las VLAN no requiere que los equipos de red se trasladen o conecten físicamente.

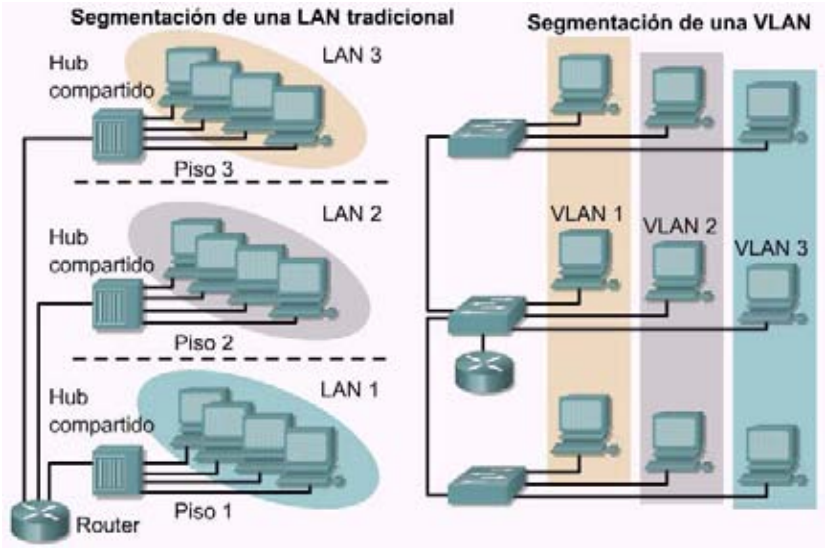

Fig. 1.20 – Las VLAN y los límites físicos

Una estación de trabajo en un grupo de VLAN se limita a comunicarse con los servidores de archivo en el mismo grupo de VLAN. Las VLAN segmentan de forma lógica la red en diferentes dominios de broadcast, de manera tal que los paquetes sólo se conmutan entre puertos y se asignan a la misma VLAN. Las VLAN se componen de hosts o equipos de red conectados mediante un único dominio de puenteo. El dominio de puenteo se admite en diferentes equipos de red. Los switches de LAN operan protocolos de puenteo con un grupo de puente separado para cada VLAN.

Las VLAN se crean para brindar servicios de segmentación proporcionados tradicionalmente por routers físicos en las configuraciones de LAN. Las VLAN se ocupan de la escalabilidad, seguridad y gestión de red. Los routers en las topologías de VLAN proporcionan filtrado de broadcast, seguridad y gestión de flujo de tráfico. Los switches no puentean ningún tráfico entre VLAN, dado que esto viola la integridad del dominio de broadcast de las VLAN. El tráfico sólo debe enrutarse entre VLAN.

1.6.2 Operación de las VLAN

Una VLAN se compone de una red conmutada que se encuentra lógicamente segmentada. Cada puerto de switch se puede asignar a una VLAN. Los puertos asignados a la misma VLAN comparten broadcasts. Los puertos que no pertenecen a esa VLAN no comparten

esos broadcasts. Esto mejora el desempeño de la red porque se reducen los broadcasts innecesarios. Las VLAN de asociación estática se denominan VLAN de asociación de puerto central y basadas en puerto. Cuando un dispositivo entra a la red, da por sentado automáticamente que la VLAN está asociada con el puerto al que se conecta.

Fig. 1.21 – VLAN estática

Los usuarios conectados al mismo segmento compartido comparten el ancho de banda de ese segmento. Cada usuario adicional conectado al medio compartido significa que el ancho de banda es menor y que se deteriora el desempeño de la red. Las VLAN ofrecen mayor ancho de banda a los usuarios que una red Ethernet compartida basada en hubs. La VLAN por defecto para cada puerto del switch es la VLAN de administración. La VLAN de administración siempre es la VLAN 1 y no se puede borrar. Por lo menos un puerto debe asignarse a la VLAN 1 para poder gestionar el switch. Todos los demás puertos en el switch pueden reasignarse a VLAN alternadas.

Las VLAN de asociación dinámica son creadas mediante software de administración de red. Se usa CiscoWorks 2000 o CiscoWorks for Switched Internetworks para crear las VLAN dinámicas. Las VLAN dinámicas permiten la asociación basada en la dirección MAC del dispositivo conectado al puerto de switch. Cuando un dispositivo entra a la red, el switch al que está conectado consulta una base de datos en el Servidor de Configuración de VLAN para la asociación de VLAN.

Fig. 1.22 – Configuración VLAN dinámicas

En la asociación de VLAN de puerto central basada en puerto, el puerto se asigna a una asociación de VLAN específica independiente del usuario o sistema conectado al puerto. Al utilizar este método de asociación, todos los usuarios del mismo puerto deben estar en la misma VLAN. Un solo usuario, o varios usuarios pueden estar conectados a un puerto y no darse nunca cuenta de que existe una VLAN. Este método es fácil de manejar porque no se requieren tablas de búsqueda complejas para la segmentación de VLAN. Los administradores de red son responsables por configurar las VLAN de forma estática y dinámica.

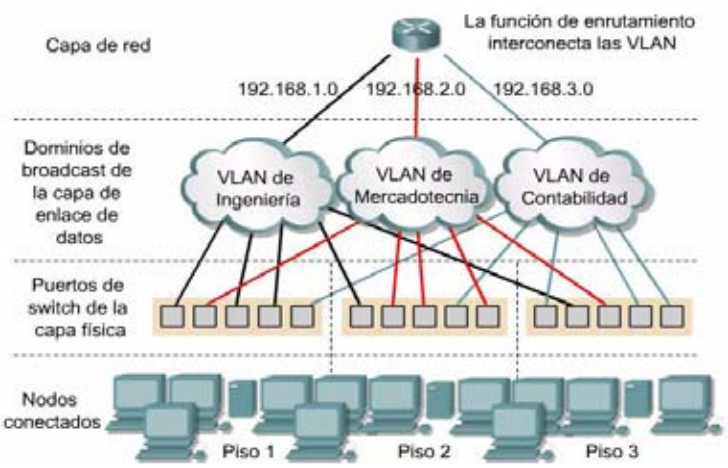

Fig. 1.23 – VLAN dinámica

Los puentes filtran el tráfico que no necesita ir a los segmentos, salvo el segmento destino. Si una trama necesita atravesar un puente y la dirección MAC destino es conocida, el puente sólo envía la trama al puerto de puente correcto. Si la dirección MAC es desconocida,

inunda la trama a todos los puertos en el dominio de broadcast, o la VLAN, salvo el puerto origen donde se recibió la trama. Los switches se consideran como puentes multipuerto.

1.6.3 Ventajas de las VLAN

Las VLAN permiten que los administradores de red organicen las LAN de forma lógica en lugar de física. Ésta es una ventaja clave. Esto permite que los administradores de red realicen varias tareas:

- Trasladar fácilmente las estaciones de trabajo en la LAN
- Agregar fácilmente estaciones de trabajo a la LAN
- Cambiar fácilmente la configuración de la LAN
- Controlar fácilmente el tráfico de red
- Mejorar la seguridad

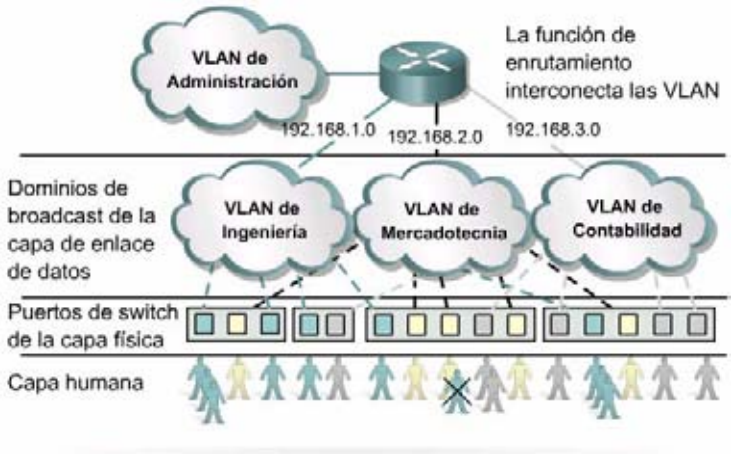

Fig. 1.24 – Ventaja de las VLAN

1.6.4 Tipos de VLAN

Existen tres asociaciones básicas de VLAN que se utilizan para determinar y controlar de qué manera se asigna un paquete:

- VLAN basadas en puerto
- VLAN basadas en direcciones MAC

- VLAN basadas en protocolo

La cantidad de VLAN en un switch varía según diversos factores:

- Patrones de tráfico
- Tipos de aplicaciones
- Necesidades de administración de red
- Aspectos comunes del grupo

El esquema de direccionamiento IP es otra consideración importante al definir la cantidad de VLAN en un switch.

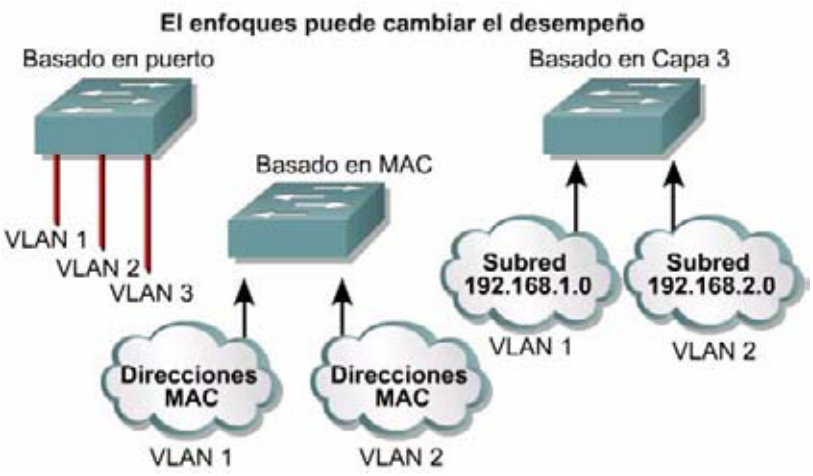

Fig. 1.25 – Tipos de VLAN

Existen dos métodos principales para el etiquetado de tramas: el enlace Inter-Switch (ISL) y 802.1Q. ISL es un protocolo propietario de Cisco y antiguamente era el más común, pero está siendo reemplazado por el etiquetado de trama estándar IEEE 802.1Q.

A medida que los paquetes son recibidos por el switch desde cualquier dispositivo de estación final conectado, se agrega un identificador único de paquetes dentro de cada encabezado. Esta información de encabezado designa la asociación de VLAN de cada paquete. El paquete se envía entonces a los switches o routers correspondientes sobre la base del identificador de VLAN y la dirección MAC. Al alcanzar el nodo destino, el ID de VLAN es

eliminado del paquete por el switch adyacente y es enviado al dispositivo conectado. El etiquetado de paquetes brinda un mecanismo para controlar el flujo de broadcasts y aplicaciones, mientras que no interfiere con la red y las aplicaciones. La emulación de LAN (LANE) es una forma en que una red de Modo de Transferencia Asíncrona (ATM) simula una red Ethernet. No hay etiquetado en LANE, pero la conexión virtual utilizada implica un ID de VLAN.

1.7 CABLEADO DE LAS LAN

1.7.1 Ethernet en el Campus

Ethernet es la tecnología LAN de uso más frecuente. Un grupo formado por las empresas Digital, Intel y Xerox, conocido como DIX, fue el primero en implementar Ethernet. DIX creó e implementó la primera especificación LAN Ethernet, la cual se utilizó como base para la especificación 802.3 del Instituto de Ingenieros Eléctrica y Electrónica (IEEE), publicada en 1980. Más tarde, el IEEE extendió la especificación 802.3 a tres nuevas comisiones conocidas como 802.3u (Fast Ethernet), 802.3z (Gigabit Ethernet transmitido en fibra óptica) y 802.3ab (Gigabit Ethernet en UTP).

Los requisitos de la red pueden forzar a la actualización a topologías de Ethernet más rápidas. La mayoría de las redes de Ethernet admiten velocidades de 10 Mbps y 100 Mbps.

La nueva generación de productos para multimedia, imagen y base de datos puede fácilmente abrumar a redes que funcionan a las velocidades tradicionales de Ethernet de 10 y 100 Mbps. Los administradores de red pueden considerar proveer Gigabit Ethernet desde el backbone hasta los usuarios finales. Los costos de instalación de un nuevo cableado y de adaptadores pueden hacer que esto resulte casi imposible. Por el momento, Gigabit Ethernet en el escritorio no constituye una instalación estándar.

Por lo general, las tecnologías Ethernet se pueden utilizar en redes de campus de muchas maneras diferentes:

- Se puede utilizar Ethernet de 10 Mbps a nivel del usuario para brindar un buen rendimiento. Los clientes o servidores que requieren mayor ancho de banda pueden utilizar Ethernet de 100 Mbps.
- Se usa Fast Ethernet como enlace entre el usuario y los dispositivos de red. Puede admitir la combinación de todo el tráfico de cada segmento Ethernet.
- Para mejorar el rendimiento cliente-servidor a través de la red campus y evitar los cuellos de botella, se puede utilizar Fast Ethernet para conectar servidores empresariales.
- A medida que se tornen económicos, se debe implementar Fast Ethernet o Gigabit Ethernet entre dispositivos backbone.

1.7.2 Medios de Ethernet y Requisitos de Conector

Antes de seleccionar la implementación de Ethernet, tenga en cuenta los requisitos de los conectores y medios para cada una de ellas. También tenga en cuenta el nivel de rendimiento que necesita la red.

Las especificaciones de los cables y conectores usados para admitir las implementaciones de Ethernet derivan del cuerpo de estándares de la Asociación de la Industria de las Telecomunicaciones (TIA) y la Asociación de Industrias Electrónicas (EIA). Las categorías de cableado definidas para Ethernet derivan del Estándar de Recorridos y Espacios de Telecomunicaciones para Edificios Comerciales EIA/TIA-568 (SP-2840).

La Figura 1.26 compara las especificaciones de los cables y conectores para las implementaciones de Ethernet más conocidas. Es importante reconocer la diferencia entre los medios utilizados para Ethernet 10 Mbps y Ethernet 100 Mbps. Las redes con una combinación de tráfico de 10 y 100 Mbps utilizan UTP Categoría 5 para admitir Fast Ethernet.

	10BASE2	10BASE5	10BASE-T	100BASE-TX	100BASE-FX	1000BASE-CX	1000BASE-T	1000BASE-SX	1000BASE-LX
Medios	Cable coaxial de 50 ohmios (Thinnet)	Cable coaxial de 50 ohmios (Thicknet)	UTP Categoría 3, 4, 5 EIA/TIA, dos pares	UTP Categoría 5 EIA/TIA, dos pares	fibra multimodo 62.5/125	STP	UTP Categoría 5 EIA/TIA, cuatro pares	fibra micro multimodo 62.5/50	fibra micro multimodo 62.5/50; fibra monomodo de 9 micrones
Longitud de segmento máxima	185 m (606,94 pies)	500 m (1.640,4 pies)	100 m (328 pies)	100 m (328 pies)	400 m (1312,3 pies)	25 m (82 pies)	100 m (328 pies)	275 m (853 pies) para microfibra 62.5; 550 m (1804,5 pies) para microfibra 50	440 m (1443,6 pies) para microfibra 62.5; 550 m (1804,5 pies) para micro fibra 50; 3 a 10 km (1,86 a 6,2 millas) para fibra monomodo
Topología	Bus	Bus	Estrella	Estrella	Estrella	Estrella	Estrella	Estrella	Estrella
Conector	BNC	Interfaz de unidad de conexión (AUI)	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)		ISO 8877 (RJ-45)	ISO 8877 (RJ-45)		

Fig. 1.26 – Especificaciones de cable y conectores para una implementación Ethernet

1.7.3 Medios de Conexión

La Figura 1.27 muestra los diferentes tipos de conexión utilizados en cada implementación de la capa física. El jack y el conector de jack registrado (RJ-45) son los más comunes.

En algunos casos el tipo de conector de la tarjeta de interfaz de red no se ajusta al medio al que se tiene que conectar. Sin embargo, puede existir una interfaz para el conector interfaz de unidad de conexión (AUI) de 15 pins. El conector AUI permite que medios diferentes se conecten cuando se usan con el transceptor apropiado. Un transceptor es un adaptador que convierte un tipo de conexión a otra. Por ejemplo, un transceptor convierte un conector AUI en uno RJ-45, coaxial, o de fibra óptica. En Ethernet 10BASE5, o Thicknet, se utiliza un cable corto para conectar el AUI a un transceptor en el cable principal.

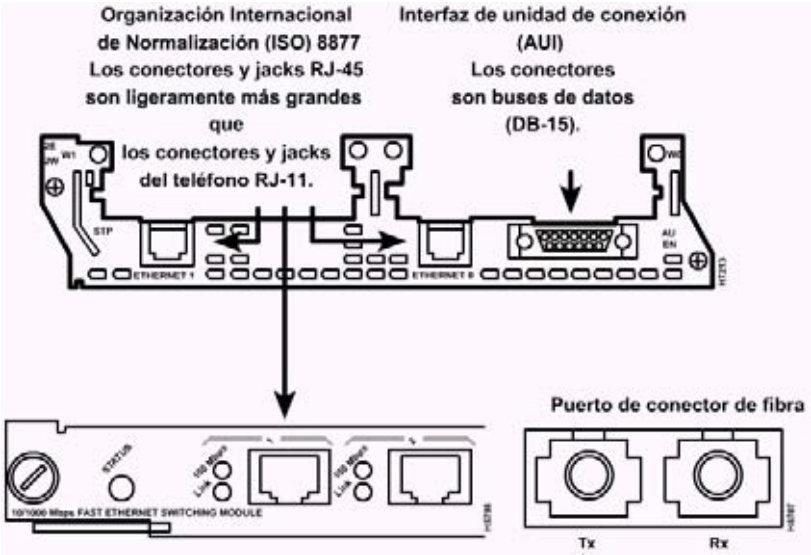

Fig. 1.27 – Diferenciación de las conexiones

1.7.4 Implementación del UTP

EIA/TIA especifica el uso de un conector RJ-45 para cables UTP. Las letras RJ significan "registered jack" (jack registrado), y el número 45 se refiere a una secuencia específica de cableado. El conector transparente RJ-45 muestra ocho hilos de distintos colores. Cuatro de estos hilos conducen el voltaje y se consideran "tip" (punta) (T1 a T4). Los otros cuatro hilos están conectados a tierra y se llaman "ring" (anillo) (R1 a R4). Tip y ring son términos que surgieron a comienzos de la era de la telefonía. Hoy, estos términos se refieren al hilo positivo y negativo de un par. Los hilos del primer par de un cable o conector se llaman T1 y R1. El segundo par son T2 y R2, y así sucesivamente.

El conector RJ-45 es el componente macho, engarzado al extremo del cable. Las ubicaciones de los pins están numeradas desde 8, a la izquierda, hasta 1, a la derecha. El jack es el componente femenino en un dispositivo de red, toma de pared o panel de conexión.

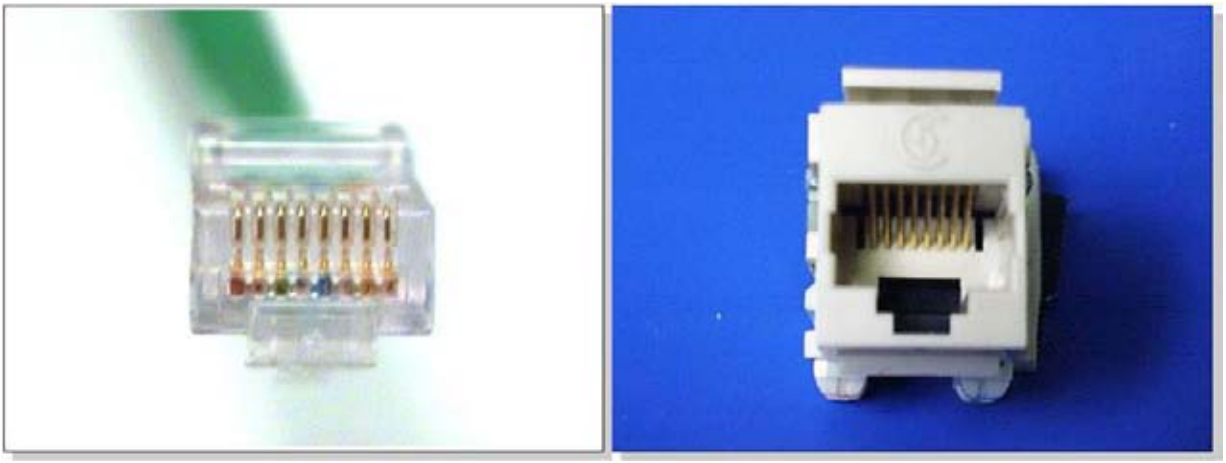

Fig. 1.28 – Conector RJ-45 hembra y macho

Para que la electricidad fluya entre el conector y el jack, el orden de los hilos debe seguir el código de colores T568A, o T568B recomendado en los estándares EIA/TIA-568-B.1. Identifique la categoría de cableado EIA/TIA correcta que debe usar un dispositivo de conexión, refiriéndose a la documentación de dicho dispositivo, o ubicando alguna identificación en el mismo cerca del jack. Si no se dispone de la documentación o de alguna identificación, use categoría 5E o mayor, dado que las categorías superiores pueden usarse en lugar de las inferiores. Así podrá determinar si va a usar cable de conexión directa (straight-through) o de conexión cruzada (crossover).

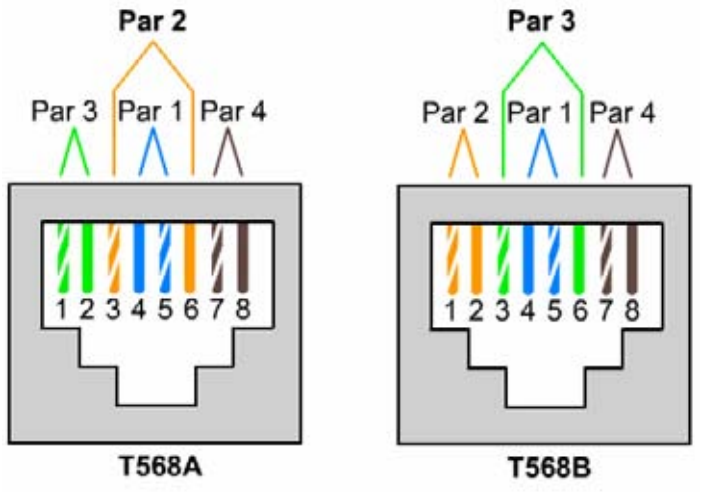

Fig. 1.29 – Estándares EIA/TIA T568A y T568B

Si los dos conectores de un cable RJ-45 se colocan uno al lado del otro, con la misma orientación, podrán verse en cada uno los hilos de color. Si el orden de los hilos de color es el mismo en cada extremo, entonces el cable es de conexión directa

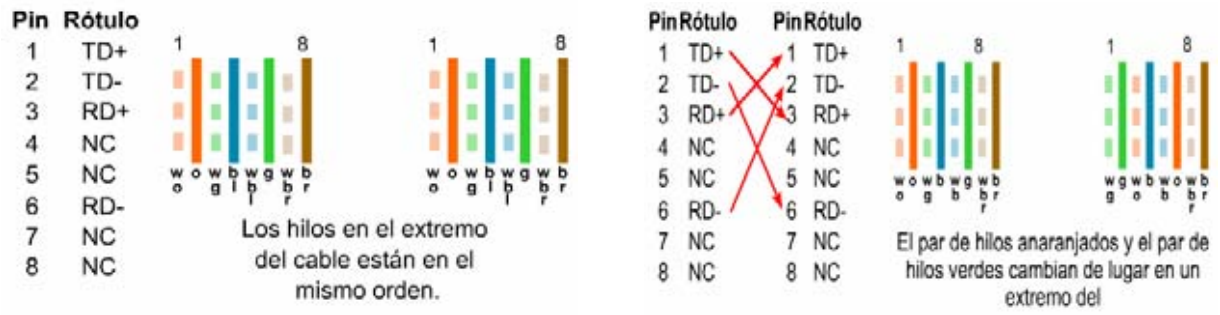

Fig. 1.30 – Implementación de UTP Conexión Directa y Cruzada

En un cable de conexión cruzada, los conectores RJ-45 de ambos extremos muestran que algunos hilos de un extremo del cable están cruzados a un pin diferente en el otro extremo del cable. Los pins 1 y 2 de un conector se conectan respectivamente a los pins 3 y 6 de otro.

Utilice cables de conexión directa para el siguiente cableado:

- Switch a router
- Switch a PC o servidor
- Hub a PC o servidor

Utilice cables de conexión cruzada para el siguiente cableado:

- Switch a switch
- Switch a hub
- Hub a hub
- Router a router
- PC a PC
- Router a PC

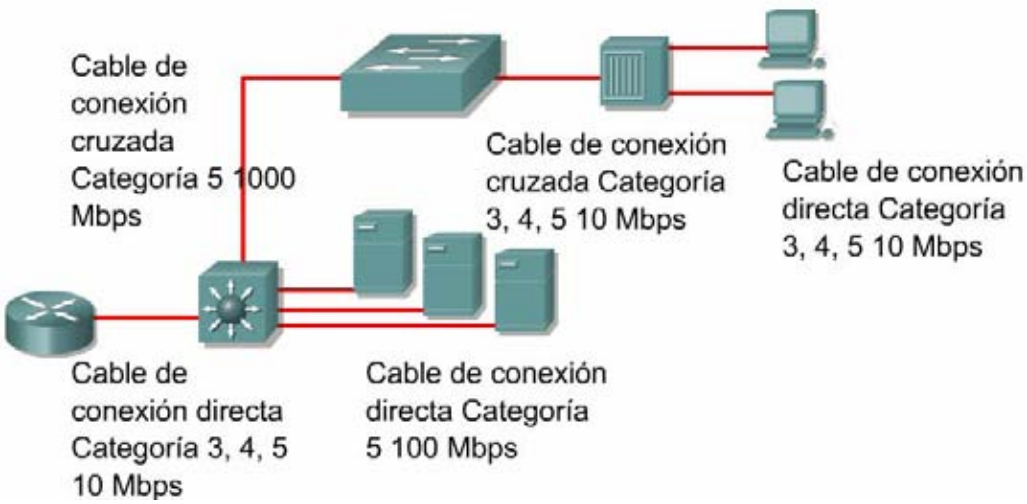

Fig. 1.31 – Tipos de cables en una conexión Ethernet

1.7.5 Repetidores

En Ethernet e IEEE 802.3 se implementa la "regla 5-4-3", en referencia al número de repetidores y segmentos en un Backbone de acceso compartido con topología de árbol. La "regla 5-4-3 divide la red en dos tipos de segmentos físicos: Segmentos Poblados (de usuarios), y Segmentos no Poblados (enlaces). En los segmentos poblados se conectan los sistemas de los usuarios. Los segmentos no poblados se usan para conectar los repetidores de la red entre si. La regla manda que entre cualquiera dos nodos de una red, puede existir un máximo de cinco segmentos, conectados por cuatro repetidores o concentradores, y solamente tres de los cinco segmentos pueden tener usuarios conectados a los mismos.

El protocolo Ethernet requiere que una señal enviada en la LAN alcance cualquier parte de la red dentro de una longitud de tiempo especificada. La "regla 5-4-3" asegura que esto pase. Cada repetidor a través del cual pasa la señal añade una pequeña cantidad de tiempo al proceso, por lo que la regla está diseñada para minimizar el tiempo de transmisión de la señal. Demasiada latencia en la LAN incrementa la cantidad de colisiones tardías, haciendo la LAN menos eficiente.

1.7.6 Hubs

El uso de un hub hace que cambie la topología de la red desde un bus lineal, donde cada dispositivo se conecta de forma directa al cable, a una en estrella. En un hub, los datos que llegan a un puerto del hub se transmiten de forma eléctrica a todos los otros puertos conectados al mismo segmento de red, salvo a aquel puerto desde donde enviaron los datos.

1.7.7 Redes Inalámbricas

Se puede crear una red inalámbrica con mucho menos cableado que el necesario para otras redes. Las señales inalámbricas son ondas electromagnéticas que se desplazan a través del aire. Las redes inalámbricas usan Radiofrecuencia (RF), láser, infrarrojo (IR), o satélite/microondas para transportar señales de un computador a otro sin una conexión de cable permanente. El único cableado permanente es el necesario para conectar los puntos de acceso de la red. Las estaciones de trabajo dentro del ámbito de la red inalámbrica se pueden trasladar con facilidad sin tener que conectar y reconectar al cableado de la red.

Una aplicación común de la comunicación inalámbrica de datos es la que corresponde a los usuarios móviles. Algunos ejemplos de usuarios móviles incluyen las personas que trabajan a distancia, aviones, satélites, las sondas espaciales remotas, naves espaciales y estaciones espaciales.

La tecnología de radiofrecuencia permite que los dispositivos se encuentren en habitaciones o incluso en edificios diferentes. El rango limitado de señales de radio restringe el uso de esta clase de red. La tecnología de RF puede utilizar una o varias frecuencias. Una radiofrecuencia única está sujeta a interferencias externas y a obstrucciones geográficas. Además, una sola frecuencia es fácil de monitorear, lo que hace que la transmisión de datos no sea segura.

1.7.8 Puentes

A veces, es necesario dividir una LAN grande en segmentos más pequeños que sean más fáciles de manejar. Esto disminuye la cantidad de tráfico en una sola LAN y puede

extender el área geográfica más allá de lo que una sola LAN puede admitir. Los dispositivos que se usan para conectar segmentos de redes son los puentes, switches, routers y gateways. Los switches y los puentes operan en la capa de enlace de datos del modelo de referencia OSI. La función del puente es tomar decisiones inteligentes con respecto a pasar señales o no al segmento siguiente de la red.

1.7.9 Switches

La conmutación es una tecnología que alivia la congestión en las LAN Ethernet, reduciendo el tráfico y aumentando el ancho de banda. Los switches pueden remplazar a los hubs con facilidad debido a que ellos funcionan con las infraestructuras de cableado existentes. Esto mejora el rendimiento con un mínimo de intrusión en la red ya existente.

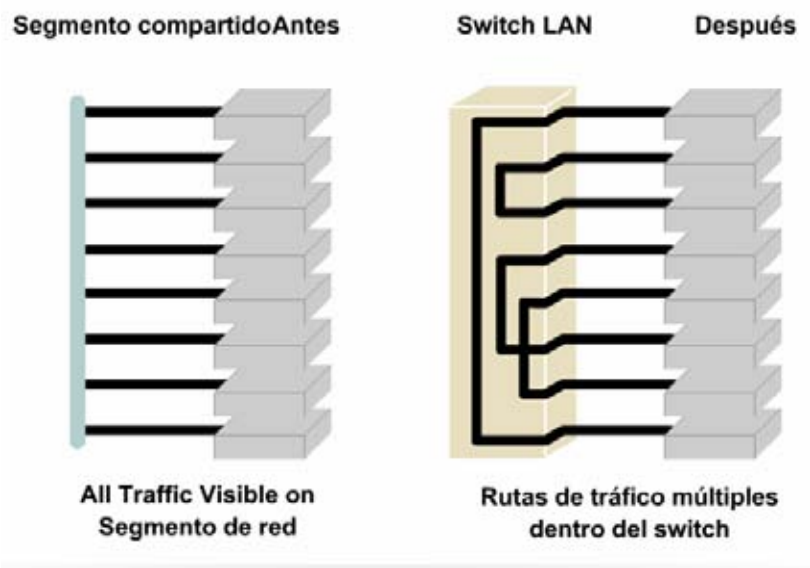

Fig. 1.32 – Micro segmentación de la red

1.8 CONSIDERACIONES DE DISEÑO LAN

La tarea de diseñar una red puede ser una tarea fascinante e implica mucho más que simplemente conectar dos computadoras entre sí. Una red requiere muchas funciones para que sea confiable, escalable y fácil de administrar. Para diseñar redes confiables, fáciles de

administrar y escalables, los diseñadores de red deben darse cuenta de que cada uno de los componentes principales de una red tiene requisitos de diseño específicos.

El diseño de red se ha vuelto cada vez más difícil a pesar de los avances que se han logrado a nivel del rendimiento de los equipos y las capacidades de los medios. El uso de distintos tipos de medios y de las LAN que se interconectan con otras redes agrega complejidad al entorno de red. Los buenos diseños de red permiten mejorar el rendimiento y reducir las dificultades asociadas con el crecimiento y la evolución de la red.

Una LAN abarca una sola habitación, un edificio o un conjunto de edificios que se encuentran cerca unos de otros. Un grupo de instalaciones cuyos edificios se encuentran ubicados a corta distancia unos de otros y que pertenecen a una sola organización se conoce como campus. Los siguientes aspectos de la red deben ser identificados antes de diseñar una LAN más amplia:

- Una *capa de acceso* que conecte los usuarios finales a la LAN.
- Una *capa de distribución* que ofrezca conectividad basada en políticas entre las LAN de usuario final.
- Una *capa núcleo* que ofrezca la conexión más rápida que sea posible entre los distintos puntos de distribución.

Cada una de estas capas de diseño de LAN requiere los switches más adecuados para realizar tareas específicas. Las características, las funciones y las especificaciones técnicas de cada switch varían en función de la capa de diseño de la LAN para la cual el switch fue creado. Para lograr el mejor rendimiento de la red, es importante comprender la función de cada capa y luego elegir el switch que mejor se adecua a los requisitos de la capa.

1.8.1 Objetivos del Diseño LAN

El primer paso en el diseño de una LAN es establecer y documentar los objetivos de diseño. Estos objetivos son específicos para cada organización o situación. Los requisitos de la mayoría de los diseños de red son:

- **Funcionalidad:** La red debe funcionar. Es decir, debe permitir que los usuarios cumplan con sus requisitos laborales. La red debe suministrar conectividad de usuario a usuario y de usuario a aplicación con una velocidad y confiabilidad razonables.
- **Escalabilidad:** La red debe poder aumentar de tamaño. Es decir, el diseño original debe aumentar de tamaño sin que se produzcan cambios importantes en el diseño general.
- **Adaptabilidad:** La red debe diseñarse teniendo en cuenta futuras tecnologías. La red no debería incluir elementos que limiten la implementación de nuevas tecnologías a medida que éstas van apareciendo.
- **Facilidad de administración:** La red debe estar diseñada para facilitar su monitoreo y administración, con el objeto de asegurar una estabilidad de funcionamiento constante.

1.9 OBTENCIÓN DE DIRECCIONES IP

1.9.1 Introducción

Un host de red necesita obtener una dirección exclusiva a nivel global para poder funcionar en Internet. La dirección MAC o física que posee el host sólo tiene alcance local, para identificar el host dentro de la red del área local. Como es una dirección de Capa 2, el Router no la utiliza para realizar transmisiones fuera de la LAN.

Las direcciones IP son las direcciones que más frecuentemente se utilizan en las comunicaciones en la Internet. Este protocolo es un esquema de direccionamiento jerárquico que permite que las direcciones individuales se asocien en forma conjunta y sean tratadas como grupos. Estos grupos de direcciones posibilitan una eficiente transferencia de datos a través de la Internet.

Los administradores de redes utilizan dos métodos para asignar las direcciones IP. Estos métodos son el estático y el dinámico. Independientemente del esquema de direccionamiento elegido, no es posible tener dos interfaces con la misma dirección IP. Dos hosts con la misma dirección IP pueden generar conflictos que hacen que ambos no puedan operar correctamente.

1.9.2 Asignación Estática de una Dirección IP

La asignación estática funciona mejor en las redes pequeñas con poca frecuencia de cambios. De forma manual, el administrador del sistema asigna y rastrea las direcciones IP para cada computador, impresora o servidor de una red interna. Es fundamental llevar un buen registro para evitar que se produzcan problemas con las direcciones IP repetidas. Esto es posible sólo cuando hay una pequeña cantidad de dispositivos que rastrear.

Los servidores deben recibir una dirección IP estática de modo que las estaciones de trabajo y otros dispositivos siempre sepan cómo acceder a los servicios requeridos. Considere lo difícil que sería realizar un llamado telefónico a un lugar que cambiara de número todos los días. Otros dispositivos que deben recibir direcciones IP estáticas son las impresoras en red, servidores de aplicaciones y routers.

1.9.3 Asignación de Direcciones RARP IP

El Protocolo de resolución inversa de direcciones (RARP) asocia las direcciones MAC conocidas a direcciones IP. Esta asociación permite que los dispositivos de red encapsulen los datos antes de enviarlos a la red. Es posible que un dispositivo de red, como por ejemplo una estación de trabajo sin disco, conozca su dirección MAC pero no su dirección IP. RARP permite que el dispositivo realice una petición para conocer su dirección IP. Los dispositivos que usan RARP requieren que haya un servidor RARP en la red para responder a las peticiones RARP.

1.9.4 Asignación de Direcciones BOOTP IP

El protocolo bootstrap (BOOTP) opera en un entorno cliente-servidor y sólo requiere el intercambio de un solo paquete para obtener la información IP. Sin embargo, a diferencia del RARP, los paquetes de BOOTP pueden incluir la dirección IP, así como la dirección de un router, la dirección de un servidor y la información específica del fabricante.

Sin embargo, un problema del BOOTP es que no se diseñó para proporcionar la asignación dinámica de las direcciones. Con el BOOTP, un administrador de redes crea un archivo de configuración que especifica los parámetros de cada dispositivo. El administrador

debe agregar hosts y mantener la base de datos del BOOTP. Aunque las direcciones se asignan de forma dinámica, todavía existe una relación exacta entre el número de direcciones IP y el número de hosts. Esto significa que para cada host de la red, debe haber un perfil BOOTP con una asignación de dirección IP en él. Dos perfiles nunca pueden tener la misma dirección IP. Es posible que estos perfiles se utilicen al mismo tiempo y esto quiere decir que dos hosts tendrían la misma dirección IP.

Un dispositivo utiliza el BOOTP para obtener una dirección IP cuando se inicializa. El BOOTP utiliza UDP para transportar los mensajes. El mensaje UDP se encapsula en un paquete IP. Un computador utiliza el BOOTP para enviar un paquete IP de broadcast a la dirección IP destino de todos unos, o sea, 255.255.255.255 en anotación decimal punteada. El servidor del BOOTP recibe el broadcast y responde en forma de broadcast. El cliente recibe una trama y verifica la dirección MAC. Si el cliente encuentra su propia dirección MAC en el campo de dirección destino y un broadcast en el campo IP destino, toma la dirección IP y la guarda junto con la otra información proporcionada por el mensaje BOOTP de respuesta.

1.9.5 Administración de Direcciones DHCP IP

El Protocolo de configuración dinámica del host (DHCP) es el sucesor del BOOTP. A diferencia del BOOTP, el DHCP permite que el host obtenga la dirección IP de forma dinámica sin que el administrador de red tenga que configurar un perfil individual para cada dispositivo. Lo único que se requiere para utilizar el DHCP es un rango definido de direcciones IP en un servidor DHCP. A medida que los hosts entran en línea, se comunican con el servidor DHCP y solicitan una dirección. El servidor DHCP elige una dirección y se la arrienda a dicho host. Con DHCP, la configuración completa de las red se puede obtener en un mensaje. Esto incluye todos los datos que proporciona el mensaje BOOTP más una dirección IP arrendada y una máscara de subred.

La principal ventaja que el DHCP tiene sobre el BOOTP es que permite que los usuarios sean móviles. Esta movilidad permite que los usuarios cambien libremente las conexiones de red de un lugar a otro. Ya no es necesario mantener un perfil fijo de cada dispositivo conectado a la red como en el caso del sistema BOOTP. La importancia de este avance del DHCP es su capacidad de arrendar una dirección IP a un dispositivo y luego reclamar dicha dirección IP para

otro usuario una vez que el primero la libera. Esto significa que DHCP puede asignar una dirección IP disponible a cualquiera que se conecte a la red.

1.9.6 Problemas en la Resolución de Direcciones

Uno de los principales problemas del networking es cómo comunicarse con los otros dispositivos de la red. En la comunicación TCP/IP, el datagrama de una red de área local debe contener tanto una dirección MAC destino como una dirección IP destino. Estas direcciones deben ser correctas y concordar con las direcciones IP y MAC destino del dispositivo host. Si no concuerdan, el host destino descartará el datagrama. La comunicación dentro de un segmento de LAN requiere de dos direcciones. Debe haber una forma de mapear las direcciones IP a MAC de forma automática. Se necesitaría demasiado tiempo si el usuario creara los mapas de forma manual. El conjunto TCP/IP cuenta con un protocolo, llamado Protocolo de resolución de direcciones (ARP), que puede obtener las direcciones MAC, de forma automática, para la transmisión local. Pueden surgir diferentes problemas cuando se manda información fuera de la LAN.

Las comunicaciones entre dos segmentos de LAN tienen una tarea extra. Tanto las direcciones IP como las MAC son necesarias para el dispositivo de enrutamiento intermedio y el host destino. TCP/IP tiene una variante en ARP llamada ARP proxy que proporciona la dirección MAC de un dispositivo intermedio para realizar la transmisión a otro segmento de la red fuera de la LAN.

1.10 SEGURIDAD

1.10.1 Firewall

Un Firewall es un dispositivo que filtra el tráfico entre redes, como mínimo dos. El firewall puede ser un dispositivo físico o un software sobre un sistema operativo. En general debemos verlo como una caja con dos o mas interfaces de red en la que se establecen una reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no. Incluso puede ir más allá y realizar modificaciones sobre las comunicaciones, como el NAT. Esa sería la definición genérica, hoy en día un firewall es un hardware especifico con un sistema operativo

o una IOS que filtra el tráfico TCP/UDP/ICMP/../IP y decide si un paquete pasa, se modifica, se convierte o se descarta. Para que un firewall entre redes funcione como tal debe tener al menos dos tarjetas de red.

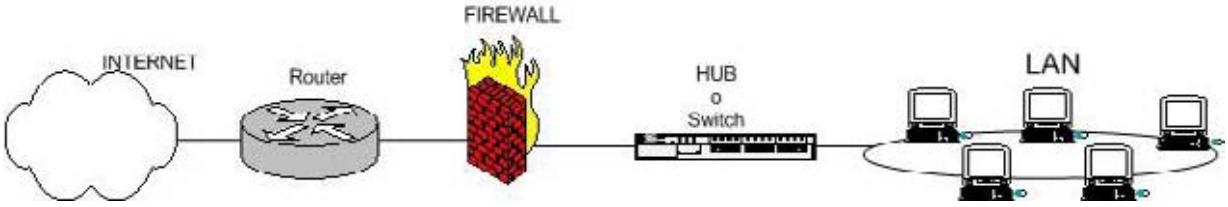

Fig. 1.33 – Firewall clásico

Dependiendo de las necesidades de cada red, puede ponerse uno o más firewalls para establecer distintos perímetros de seguridad en torno a un sistema. Es frecuente también que se necesite exponer algún servidor a internet (como es el caso de un servidor web, un servidor de correo, etc.), y en esos casos obviamente en principio se debe aceptar cualquier conexión a ellos. Lo que se recomienda en esa situación es situar ese servidor en lugar aparte de la red, el que denominamos DMZ o zona desmilitarizada. El firewall tiene entonces tres entradas:

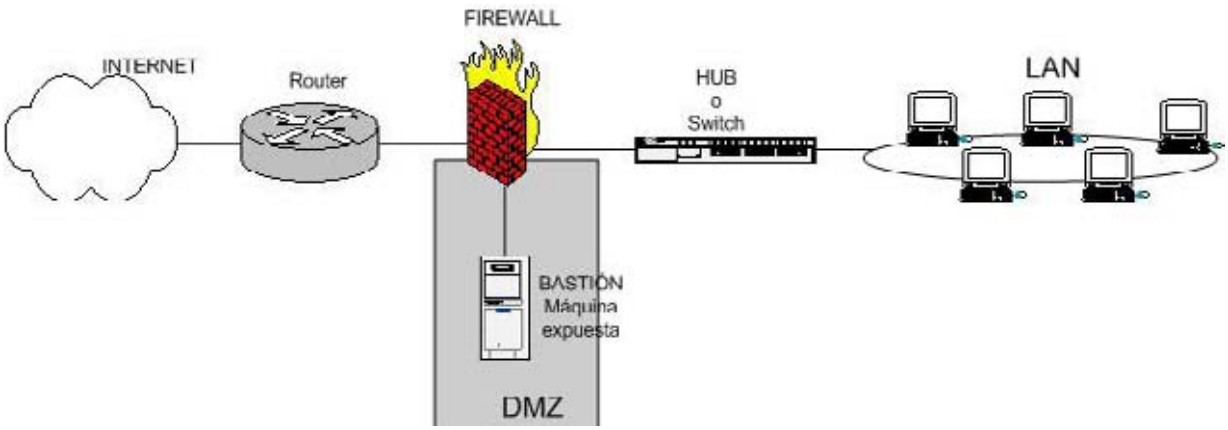

Fig. 1.34 – Zona DMZ

En la zona desmilitarizada se pueden poner tantos servidores como se necesiten. Con esta arquitectura, permitimos que el servidor sea accesible desde Internet de tal forma que si es atacado y se gana acceso a él, la red local sigue protegida por el firewall. Esta estructura de DMZ puede hacerse también con un doble firewall (aunque como se ve se puede usar un único dispositivo con al menos tres interfaces de red).

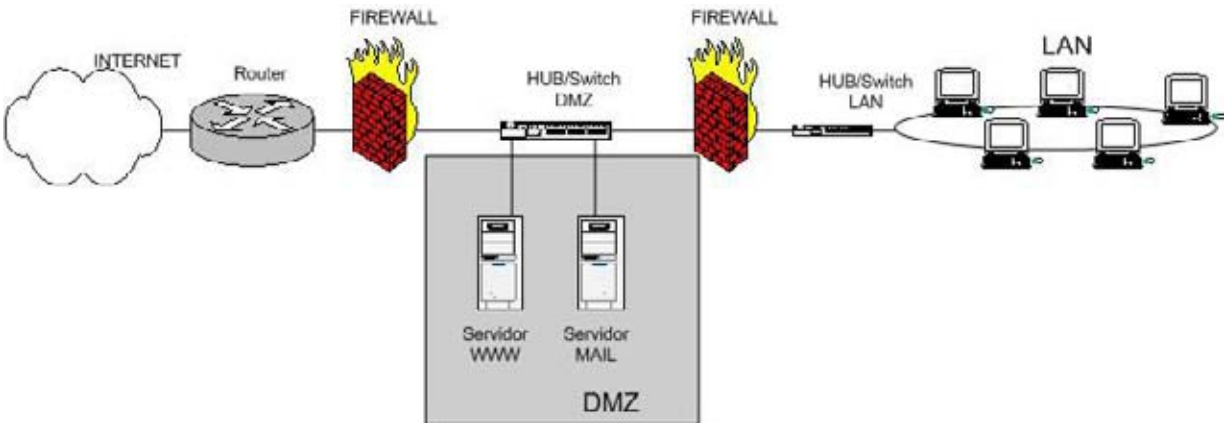

Fig. 1.35 – Zona DMZ con doble Firewall

Los firewalls se pueden usar en cualquier red. Es habitual tenerlos como protección de Internet en las empresas, aunque ahí también suelen tener una doble función: controlar los accesos externos hacia dentro y también los internos hacia el exterior; esto último se hace con el firewall o frecuentemente con un proxy (que también utilizan reglas, aunque de más alto nivel). También, en empresas de hosting con muchos servidores alojados, lo normal es encontrarnos uno o más firewalls, ya sea filtrando toda la instalación o parte de ella.

El tipo de firewall generalmente no tendrá mas que un conjunto de reglas en las que se examina el origen y destino de los paquetes del protocolo TCP/IP. En cuanto a protocolos es probable que sean capaces de filtrar muchos tipos de ellos, no solo los TCP, también los UDP, los ICMP, los GRE y otros protocolos vinculados a VPNS

Un firewall en definitiva lo que se hace es:

- Habilita el acceso a puertos de administración a determinadas IPs privilegiadas.
- Enmascara el trafico de la red local hacia el exterior (NAT, una petición de un pc de la LAN sale al exterior con la IP pública), para poder salir a internet.
- Deniega el acceso desde el exterior a puertos de administración y a todo lo que este entre 1 y 1024.

Hay dos maneras de implementar un firewall:

- Política por defecto ACEPTAR: en principio todo lo que entra y sale por el firewall se acepta y solo se denegará lo que se diga explícitamente.
- Política por defecto DENEGAR: todo esta denegado, y solo se permitirá pasar por el firewall aquellos que se permita explícitamente.

Como es obvio imaginar, la primera política facilita mucho la gestión del firewall, ya que simplemente nos tenemos que preocupar de proteger aquellos puertos o direcciones que sabemos que nos interesa; el resto no importa tanto y se deja pasar. El único problema que podemos tener es que no controlemos que es lo que esta abierto, o que en un momento dado se instale un software nuevo que abra un puerto determinado, o que no sepamos que determinados paquetes ICMP son peligrosos. Si la política por defecto es ACEPTAR y no se protege explícitamente, nos la estamos jugando un poco. En cambio, si la política por defecto es DENEGAR, a no ser que lo permitamos explícitamente, el firewall se convierte en un auténtico MURO infranqueable. El problema es que es mucho más difícil preparar un firewall así, y hay que tener muy claro como funciona el sistema y que es lo que se tiene que abrir sin caer en la tentación de empezar a meter reglas super-permisivas. Esta configuración de firewall es la recomendada, aunque no es aconsejable usarla si no se domina mínimamente el sistema.

1.10.2 IPTABLES

IPTABLES es un sistema de firewall vinculado al Kernel de Linux que se ha extendido enormemente a partir del kernel 2.4 de este sistema operativo. Al igual que el anterior sistema Ipchains, un firewall de Iptables no es como un servidor que lo iniciamos o detenemos o que se pueda caer por un error de programación. IPTABLES esta integrado con el Kernel, es parte del sistema operativo. Lo que se hace es aplicar reglas. Para ellos se ejecuta el comando iptables, con el que añadimos, borramos, o creamos reglas. Por ello un firewall de iptables, no es sino un simple script de shell en el que se van ejecutando las reglas de firewall. En algunas distribuciones de Linux, como RedHat, viene incorporado el modulo IPTABLES.

1.10.3 NAT

La Traducción de Direcciones de Red, o NAT (Network Address Translation), es un sistema que se utiliza para asignar una red completa (o varias redes) a una sola dirección IP.

NAT es necesario cuando la cantidad de direcciones IP que nos haya asignado nuestro proveedor de Internet sea inferior a la cantidad de ordenadores que queramos que accedan a Internet.

NAT nos permite aprovechar los bloques de direcciones reservadas que se describen en el RFC1918. Generalmente, una red interna se suele configurar para que use uno o más de estos bloques de red. Estos bloques son:

- 10.0.0.0/8 (10.0.0.0 - 10.255.255.255)
- 172.16.0.0/12 (172.16.0.0 - 172.31.255.255)
- 192.168.0.0/16 (192.168.0.0 - 192.168.255.255)

Un sistema Linux configurado para NAT tendrá como mínimo dos adaptadoras de red, una para Internet y la otra para la red interna. NAT se encargará de traducir los requerimientos desde la red interna, de modo que parezca que todos provienen del sistema Linux en el que se encuentra configurado NAT.

1.10.3.1 Funcionamiento de NAT

Cuando un cliente en la red interna contacta con un máquina en Internet, envía paquetes IP destinados a esa máquina. Estos paquetes contienen toda la información de direccionamiento necesaria para que puedan ser llevados a su destino. NAT se encarga de estas piezas de información:

- Dirección IP de origen (por ejemplo, 192.168.1.35)
- Puerto TCP o UDP de origen (por ejemplo, 2132)

Cuando los paquetes pasan a través de la pasarela de NAT, son modificados para que parezca que se han originado y provienen de la misma pasarela de NAT. La pasarela de NAT registra los cambios que realiza en su tabla de estado, para así poder:

- Invertir los cambios en los paquetes devueltos, y

- Asegurarse de que los paquetes devueltos pasen a través del cortafuegos y no sean bloqueados.

Podrían ocurrir los siguientes cambios:

- IP de origen: sustituida con la dirección externa de la pasarela (por ejemplo, 24.5.0.5)
- Puerto de origen: sustituido con un puerto no en uso de la pasarela, escogido aleatoriamente (por ejemplo, 53136)

Ni la máquina interna ni el anfitrión de Internet se dan cuenta de estos pasos de traducción. Para la máquina interna, el sistema NAT es simplemente una pasarela a Internet. Para el anfitrión de Internet, los paquetes parecen venir directamente del sistema NAT; ni siquiera se da cuenta de que existe la estación interna.

Cuando el anfitrión de Internet responde a los paquetes internos de la máquina, los direcciona a la IP externa de la pasarela de NAT (24.5.0.5) y a su puerto de traducción (53136). La pasarela de NAT busca entonces en la tabla de estado para determinar si los paquetes de respuesta concuerdan con alguna conexión establecida. Entonces encontrará una única concordancia basada en la combinación de la dirección IP y el puerto, y esto indica a PF que los paquetes pertenecen a una conexión iniciada por la máquina interna 192.168.1.35. Acto seguido PF realiza los cambios opuestos a los que realizó para los paquetes salientes, y reenvía los paquetes de respuesta a la máquina interna. La traducción de paquetes ICMP ocurre de forma parecida, pero sin la modificación del puerto de origen.

CAPITULO II : ESTADO DE LA RED ACTUAL

2.1 REUNA2

En 1997 surgió la iniciativa de crear una red separada para las universidades miembros del Consorcio REUNA, lo que dio paso al proyecto REUNA2.

Las universidades que por su quehacer natural desarrollan investigación en distintos campos del conocimiento, tienen un comportamiento mucho más proactivo frente a las nuevas tecnologías, productos y servicios emergentes. Lo anterior se traduce, entre otras cosas, en un mayor consumo de ancho de banda en comparación con los demás clientes de los servicios Internet.

REUNA2 no sólo es una plataforma tecnológica para entregar los servicios de Internet tradicionales (correo electrónico, transferencia de archivos, navegación por Internet, etc.) de mejor forma; sino que también permite la incorporación de nuevos servicios de banda ancha orientados a mejorar el trabajo y la investigación colaborativa, (videoconferencias masiva intersalas, videoconferencia entre dos o más usuarios) y a modernizar los actuales métodos de enseñanza (educación a distancia interactiva, video a pedido, etc.).

Además, la nueva red es un laboratorio de investigación de nuevos servicios, aplicaciones y protocolos que emerjan en el mercado, o desde los grupos de desarrollo al interior de las empresas representadas por los distribuidores locales. La idea es lograr un período de maduración de estos productos en un escenario precompetitivo.

2.1.1 La Red ATM y su Topología

REUNA2 es una red ATM a 155 Mbps, que para su comprensión se puede dividir en "la troncal" y "los accesos". La troncal de la red se basa en diez conmutadores ATM LS1010 de Cisco, interconectados mediante la red de transporte SDH de CTC Mundo.

Los accesos (universidades miembros del Consorcio REUNA) consisten en un conjunto de switches ATM LS1010 y Router 7204, ambos de Cisco, interconectados vía fibra óptica al equipo de backbone correspondiente.

Esta red permite brindar servicios de Banda Ancha (ATM nativo) a las universidades, además de servicios tradicionales (IP), lo que implica que se debe garantizar la interacción de ambos niveles de protocolo, así como aplicar controles de calidad en ambas capas, para garantizar o controlar los servicios prestados.

También hay una plataforma de administración y monitoreo centralizada que permite realizar modificaciones cuando se requieren en forma remota, además de recibir alertas y estadísticas del comportamiento de la red.

2.2 RED-UACH

Investigación y docencia son los fines fundamentales de uso de la Red de la Universidad Austral de Chile. La red corporativa data de 1995 y fue construida para dar servicios de Internet a la comunidad universitaria y como plataforma de investigación de nuevas tecnologías. Interconectada a la red de alta velocidad REUNA2 desde 1999, hoy opera sobre ella un nodo troncal de experimentación IPv6 e Internet2.

La Red UACh, inicialmente construida con tecnología ATM a 155 Mbps, en una topología anillo entregó una velocidad de acceso para el usuario final de 10 Mbps, interconectando los Campus Isla Teja, Campus Miraflores, y otras unidades ubicadas en otras ciudades sedes de la UACh. Sin embargo, la capacidad de procesamiento de tráfico alcanzó su nivel máximo. Además, no permitía algunas funcionalidades como la administración del ancho de banda generado por nuevas aplicaciones en desarrollo (QoS). Producto de esto, se hizo necesario la emigración a una nueva tecnología para el 2005.

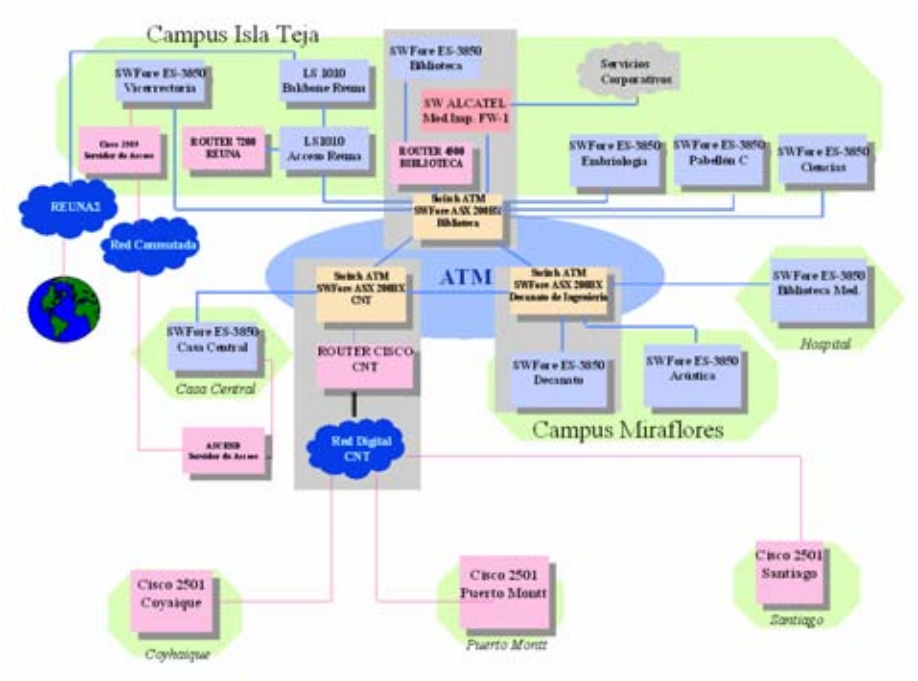

Fig. 2.1 – Red UACh ATM 155 Mbps

El backbone de la Red UACh construido con tecnología Gigabit Ethernet de 1000 Mbps brinda una velocidad de acceso para usuario final de 10/100 Mbps. Implementado con tecnología de punta posee gran capacidad de procesamiento de tráfico, funcionalidades de calidad de servicio y seguridad, flexibilidad y capacidad de crecimiento. Con esta nueva tecnología aumenta significativamente la cobertura utilizando variadas tecnologías (Fibra Óptica, Tecnologías Inalámbricas, ADSL), proporcionando acceso expedito y seguro a la red en todas las dependencias universitarias incluyendo las unidades periféricas de la UACh (aquellas que no están dentro de los campus) las que se verán beneficiadas con esta mejor conectividad.

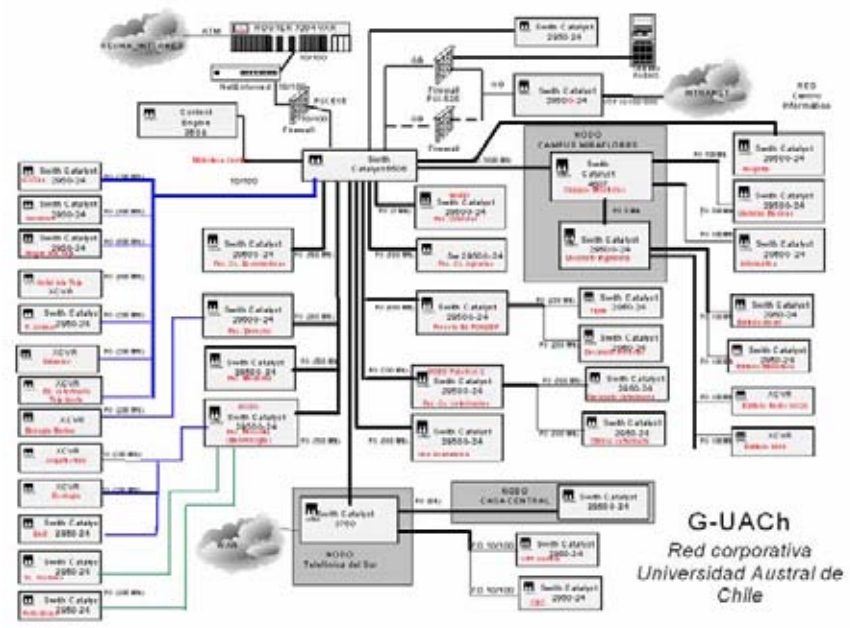

Fig. 2.2 – Red Gigabit Ethernet UACh

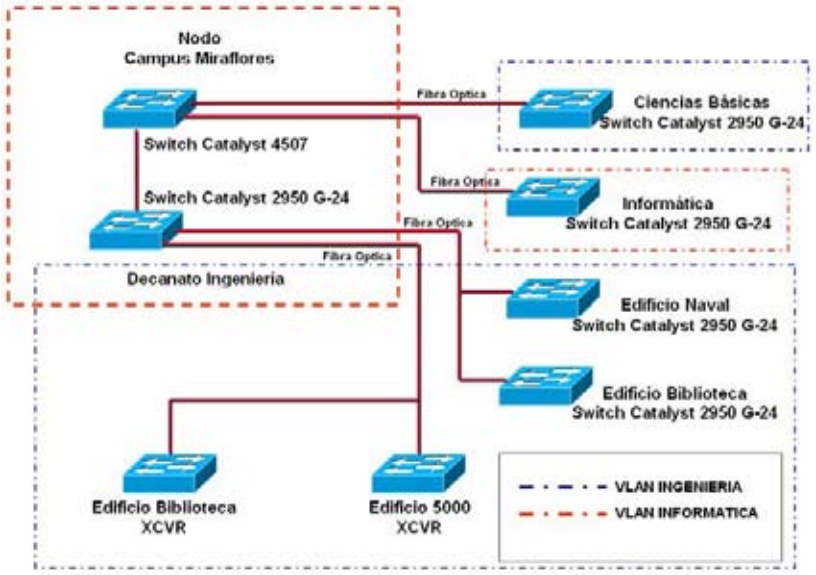

Fig. 2.3 – Topología de la Red Campus Miraflores

2.3 RED DEL INSTITUTO DE ELECTRICIDAD Y ELECTRÓNICA

2.3.1 Topología de Red

Para tener acceso a los servicios de la red corporativa, cada unidad de la casa de estudios, debe proveerse de su propio equipamiento de interconexión al backbone principal. En algunas circunstancias, se utiliza hardware obsoleto los que producen cuellos de botella disminuyendo el rendimiento de la red. A esto se suma el incremento de estaciones de trabajo en cada unidad.

El siguiente esquema describe la topología de la Red del Instituto de Electricidad y Electrónica interconectado al backbone Gigabit Ethernet.

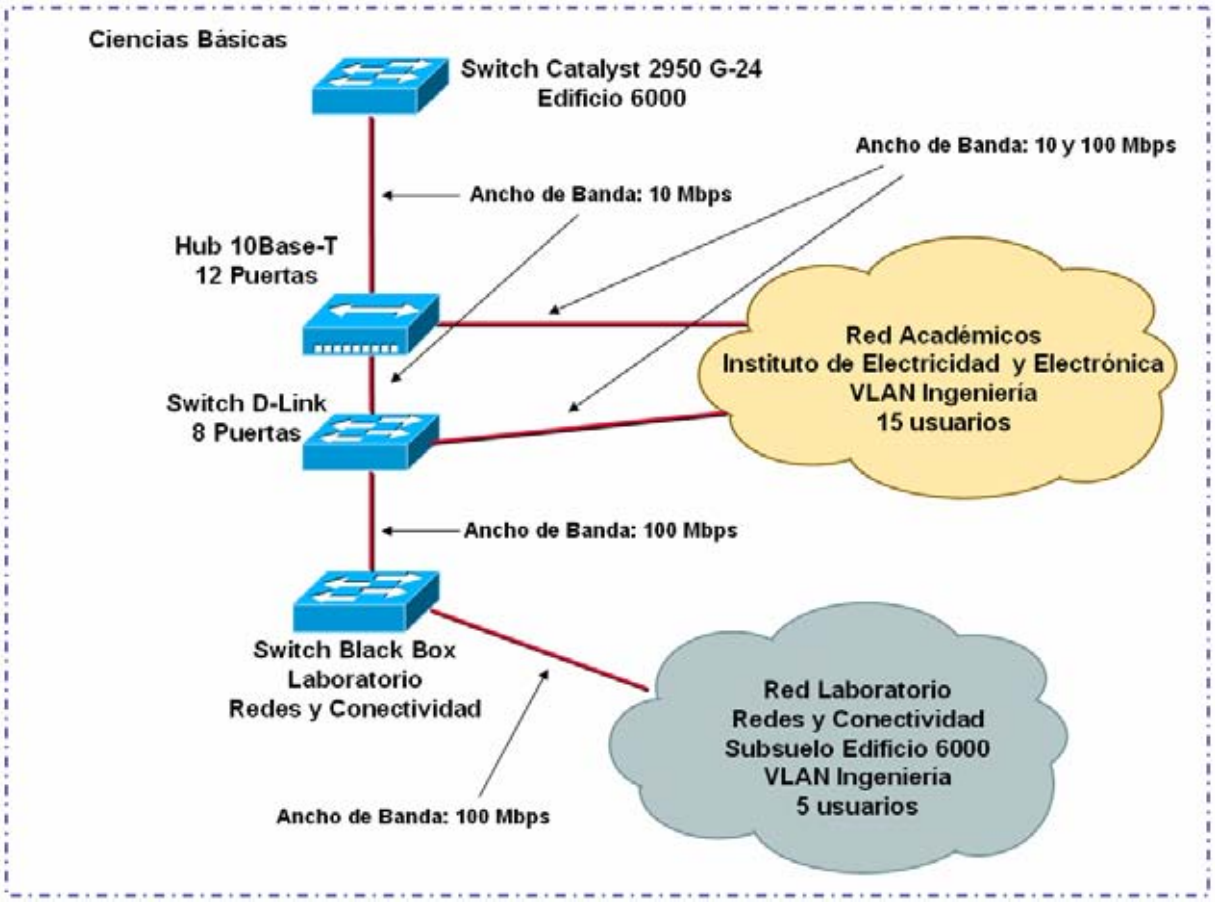

Fig. 2.4 – Red Instituto de Electricidad y Electrónica

2.4 HARDWARE EXISTENTE EN EL INSTITUTO DE ELECTRICIDAD Y ELECTRÓNICA

2.4.1 Hardware Académicos (2º Piso Edificio 6000).

Cantidad	*Hardware*
15	Estaciones de Trabajo, PC.
01	Switch Cisco Catalyst 2950-24, 10Base-T/100Base-TX, 24 Port.
-	Software, Windows 95, 98, 2000 y XP.
-	Cableado UTP Cat 5e.

Tabla 2.1 – Hardware existente en Instituto de Electricidad y Electrónica

2.4.2 Hardware Laboratorio Redes y Conectividad (Subsuelo Edificio 6000).

Cantidad	*Hardware*
01	Rack BlackBox, RM162A.
01	Patch Panel, Leviton Cat 5e, Gigamax Universal.
01	Hub Ethernet, SNMP-M12, 10Base-T, 12-Port.
01	Hub Centrecom, 3612TR, IEEE802.3/Ethernet, 10Base-T, 12 Port.
01	Switch BlackBox, Pure Networking, 10/100 Ethernet 16 Port.
01	Switch D-Link DSS-8, 10/100 Fast Ethernet, 8 Port.
03	Switch ATM-Ethernet, ForeRunner ES-3850.
01	Switch ATM, ForeRunner ASX-200BX, STM-1 155 Mbps.
01	Router Cisco, 4000 Series, 4 Ethernet – 1 ATM.
02	Terminales VT100, Hewlett Packard, HP-700/96.
01	Servidor, SUN, Netra, UltraSparc Driven
01	Digital Data Storage SUN.
01	Servidor, Hewlett Packard, NetServer 5/100 LH, Pentium 100 MHz.
01	Disk Array with Autoraid, Hewlett Packard, A3515A.

01	Disk Array, Hewlett Packard, 3231A.
02	Servidores, Hewlett Packard, D Class 9000.
01	Servidor Web, Pentium 4, 1800 MHz, 512 Mb RAM – Red Hat Linux 9.
03	Estaciones de Trabajo, Pentium 4, 1800 MHz, 512 Mb RAM.
04	Estaciones de Trabajo, Hewlett Packard, Vectra, VL-Series 3 5/75, Pentium 75MHz.
01	Servidor, Silicon Graphics CHALENG.
01	Estación de Trabajo, Silicon Graphics, INDY.
-	Software, Windows 95, 98, 2000 y XP, Red Hat Linux 9, HP-UX Install and Core 10.20.
-	Cableado UTP Cat 5e.

Tabla 2.2 – Hardware existente en Laboratorio Redes y Conectividad

2.5 DIRECCIONES IP DISPONIBLES

El direccionamiento lógico de Capa 3 en una red LAN debe ser planificado, administrado y documentado. Incluso si se cuenta con un sistema que asigne direcciones IP en forma dinámica. Esto debe hacerse con el propósito de evitar que se dupliquen las direcciones IP y evitar el uso de direcciones ilegales, pues estas no son enrutables en Internet. Además, se deben identificar claramente los nodos servidores, con el fin de aplicar medidas especiales de seguridad en los niveles superiores.

La Red de la Universidad Austral de Chile cuenta con un pool de direcciones IP públicas y que son administradas por el Centro Informático. El segmento asignado a la VLAN Ingeniería del Campus Miraflores es la subred 200.2.114.0/24.

El Instituto de Electricidad y Electrónica cuenta con 26 direcciones IP públicas que deben ser administradas y asignadas de manera óptima.

2.6 ANÁLISIS DE TRÁFICO EN REDES IP

2.6.1 Análisis de Tráfico

En redes basadas en la tecnología Ethernet clásica de bus compartido, el análisis del tráfico de red se basa habitualmente en la utilización de sondas con interfaz Ethernet conectadas al bus. Dichas sondas, con su interfaz Ethernet funcionando capturan el tráfico a analizar y constituyen la plataforma en la que se ejecutarán aplicaciones propietarias o de dominio público, con las que se podrá determinar el tipo de información que circula por la red y el impacto que pudiera llegar a tener sobre la misma. Así por ejemplo podríamos determinar la existencia de virus o el uso excesivo de aplicaciones p2p que comúnmente degradan las prestaciones de la red, sobre todo si hablamos de los enlaces principales que dan acceso a Internet. En las redes modernas basadas en conmutadores (switches), la sonda deberá conectarse a cada conmutador.

2.6.2 Analizador de Protocolo

Un analizador de protocolos es una herramienta que hace un seguimiento a las estadísticas de la red. Puede capturar tramas erróneas y aislar su fuente (las tramas de datos son paquetes de información transmitidos como una unidad sobre una red. Son definidas por el nivel de enlace de datos de la red y sólo existen en los cables que conectan los nodos de la red). Un analizador de protocolos puede ser útil para una compañía que dispone de una red grande con una plantilla altamente cualificada.

2.6.3 Analizador de Protocolo Etherpeek Versión 5.0.0

En el desarrollo de este trabajo, realizaron pruebas de laboratorios monitoreando el tráfico de la red existente en el Instituto de Electricidad y Electrónica. Se realizaron capturas de tráfico y su análisis se efectuó con el programa Etherpeek versión 5.0.0, de WildPackets.

EtherPeek es un analizador del protocolo que ofrece el diagnóstico y descifra todos los problemas de los datos que transitan la red en tiempo real durante captura. Diseñado para analizar problemas en el hardware que utiliza una red, por ejemplo, servidores, ruteadores,

estaciones de trabajo, entre otros, tiene además la cualidad de detectar si los problemas de comunicación de la red, tienen que ver con el consumo de ancho de banda, con el uso de las aplicaciones o con los datos que transitan por la red.

2.6.3.1 Estadísticas de Nodos

La ventana de estadísticas de nodos muestra el conteo de paquetes y volúmenes de tráfico en tiempo real, enviados y recibidos, por cada nodo o dispositivo en la red. Adicionalmente, muestra el total de direcciones físicas y el total de direcciones lógicas asociadas a esa dirección física.

Como resultado de una captura en un periodo de tiempo de 6 horas continuas se obtuvo un total de 79.996 paquetes, con un total de 10.706.634 bytes enviados contando un total de 303 nodos.

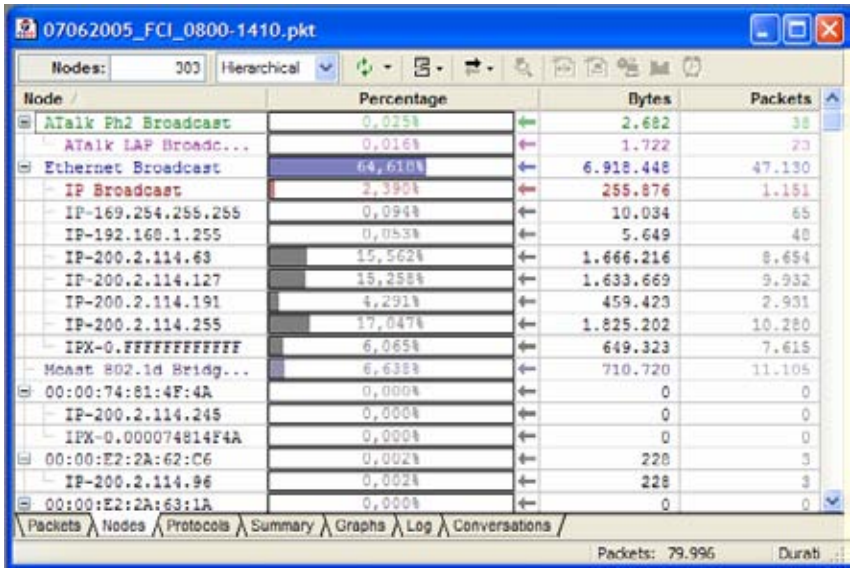

Fig. 2.5 – Estadísticas de nodos

2.6.3.2 Estadísticas de Protocolo

Esta herramienta muestra el volumen de tráfico en la red, en paquetes y bytes, analizado por protocolos y subprotocolos. Los resultados a esta prueba arrojan que el 73,337% del tráfico

son paquetes con encabezamiento IP y un 8,122% de paquetes de protocolos NetBEUI/NetBIOS.

Total Packets: 79.996
Total Bytes: 10.706.634
Protocols: 91

Protocol	Percentage	%	Bytes	Packets
Ethernet Type 2		0.000%	0	0
IP		73.337%	7.851.917	48.138
ARP		3.790%	405.824	6.341
IPX		0.568%	60.808	948
IEEE 802.3		0.000%	0	0
802.1 Spanning Tree		6.638%	710.720	11.105
NetBEUI/NetBIOS		8.122%	869.560	5.415
IPX-LSAP		4.363%	467.135	4.777
IPX		0.569%	60.906	949
IPX-SNAP		0.565%	60.474	941
Cisco Discovery		1.441%	154.336	371
AppleTalk		0.016%	1.722	23
AARP		0.009%	960	15
SNAP-00-00-0C-20-04		0.443%	47.424	741
Null SAP		0.139%	14.848	232

Tabla 2.3 – Estadísticas de protocolo

2.6.3.3 Resumen Estadístico

Esta herramienta permite visualizar monitorear las estadísticas de la red en tiempo real y guardar esta la información para una posterior comparación. Las estadísticas son acumulativas del periodo de captura. Permite visualizar parámetros importantes como el total de información enviada, total de paquetes, total de paquetes de broadcast, total de paquetes de multicast, errores en la red, etc.

Duration: 06:10:20

Group	Stat	Bytes	Packets	B/sec	P/sec	% of B	% of P
General	Start Date	06/07/2005	06/07/2005	06/07/2005	06/07/2005	06/07/2005	06/07/2005
General	Start Time	08:00:31	08:00:31	08:00:31	08:00:31	08:00:31	08:00:31
General	Duration	06:10:20	06:10:20	06:10:20	06:10:20	06:10:20	06:10:20
General	Total Bytes	10.706.634	-	481,831	-	100.000%	-
General	Total Packets	-	79.996	-	3,600	-	100.000%
General	Total Broadcast	6.918.448	47.130	311,351	2,121	64.618%	58.915%

Group	Stat	Bytes	Packets	B/sec	P/sec	% of B	% of P
General	Total Multicast	2.234.056	23.050	100,539	1,037	20.866%	28.814%
General	Average Utilization (kbits/s)	4,085	4,085	4,085	4,085	4,085	4,085
Errors	Total	-	0	-	0,000	-	0.000%
Errors	CRC	-	0	-	0,000	-	0.000%
Errors	Frame Alignment	-	0	-	0,000	-	0.000%
Errors	Runt	-	0	-	0,000	-	0.000%
Errors	Oversize	-	0	-	0,000	-	0.000%
Counts	Physical Addresses Seen	125	125	125	125	125	125
Counts	AppleTalk Addresses Seen	2	2	2	2	2	2
Counts	IP Addresses Seen	160	160	160	160	160	160
Counts	DECnet Addresses Seen	0	0	0	0	0	0
Counts	Protocols Seen	91	91	91	91	91	91
Counts	IPX Addresses Seen	14	14	14	14	14	14
Size Distribution	<= 64	-	25.180	-	1,133	-	31.477%
Size Distribution	65-127	-	30.122	-	1,356	-	37.654%
Size Distribution	128-255	-	21.478	-	0,967	-	26.849%
Size Distribution	256-511	-	2.701	-	0,122	-	3.376%
Size Distribution	512-1023	-	97	-	0,004	-	0.121%
Size Distribution	1024-1517	-	377	-	0,017	-	0.471%
Size Distribution	>= 1518	-	41	-	0,002	-	0.051%

Tabla 2.4 – Resumen estadístico

2.6.3.4 Gráficos

Esta herramienta permite visualizar de forma gráfica las estadísticas entregadas. Por ejemplo, el tamaño de las tramas, velocidad de transferencia, promedio de uso de la red, comparación de broadcasts versus información, errores en la red, etc.

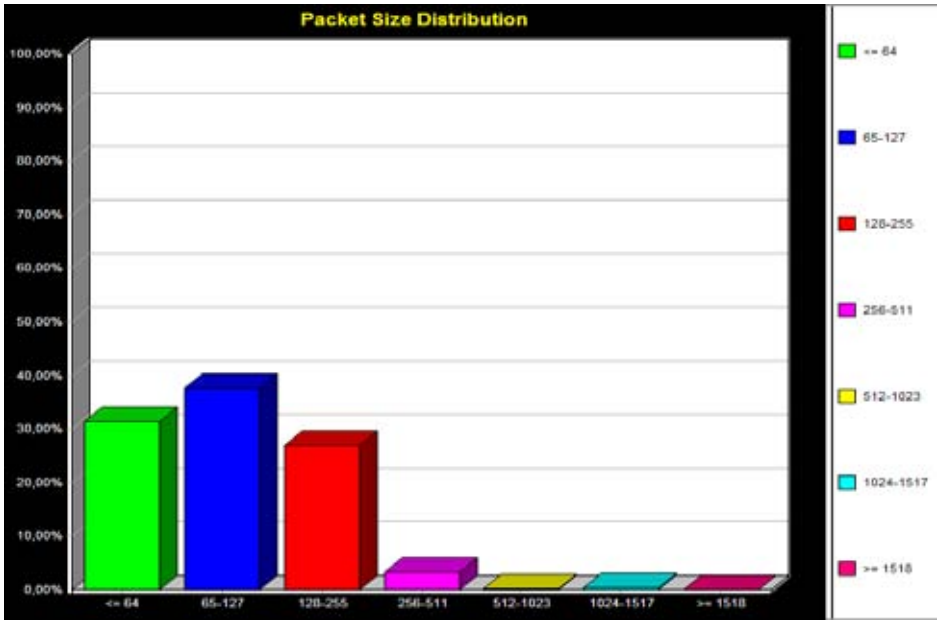

Fig. 2.6 – Distribución de tamaño de paquetes

CAPITULO III : PROPUESTA DE MEJORAMIENTO DE LA RED ACTUAL

3.1 REQUERIMIENTOS

La necesidad de mejorar la red actual surge a partir del crecimiento del uso de computadores como herramienta de apoyo al trabajo. Así mismo, el uso de computadores también se hace cada día más necesario como ayuda para el aprendizaje, pues existen asignaturas en donde ya es de carácter obligatorio el uso de ésta herramienta. Sin embargo, el crecimiento de la población de computadores demanda números IP y número de conexiones de acceso a la red, lo que de otro punto de vista, desencadena en un aumento de tráfico de paquetes en la red. Otro aspecto es la carencia de políticas de seguridad desde el interior de la red universitaria, con lo que cada nodo en la red no es inmune a ataques informáticos.

Por otro lado, el Instituto de Electricidad y Electrónica cuenta con nuevo equipamiento de tecnología ATM, transferido desde el Centro Informático en el desarrollo de esta tesis, el que fortalece enormemente el Laboratorio de Redes y Conectividad potenciando la actividad académica. Con estos equipos, se creará una red ATM piloto integrada a la nueva red Gigabit Ethernet, facilitando enormemente el aprendizaje y comprensión de los conceptos de conectividad, dándole un sello especial a los alumnos de las carreras de ingeniería de la Universidad Austral de Chile.

3.2 PROPUESTA DE MEJORAMIENTO DE LA RED ACTUAL

El modelo de red que se propone para mejorar el actual, consiste en una nueva topología, esta consiste en implementar una red conmutada interconectada al backbone UACh. Para tener una mayor funcionalidad de estos equipos deben poseer la misma tecnología existente en la red de la Universidad Austral de Chile.

En el siguiente esquema se plantea de forma general el modelo a realizar:

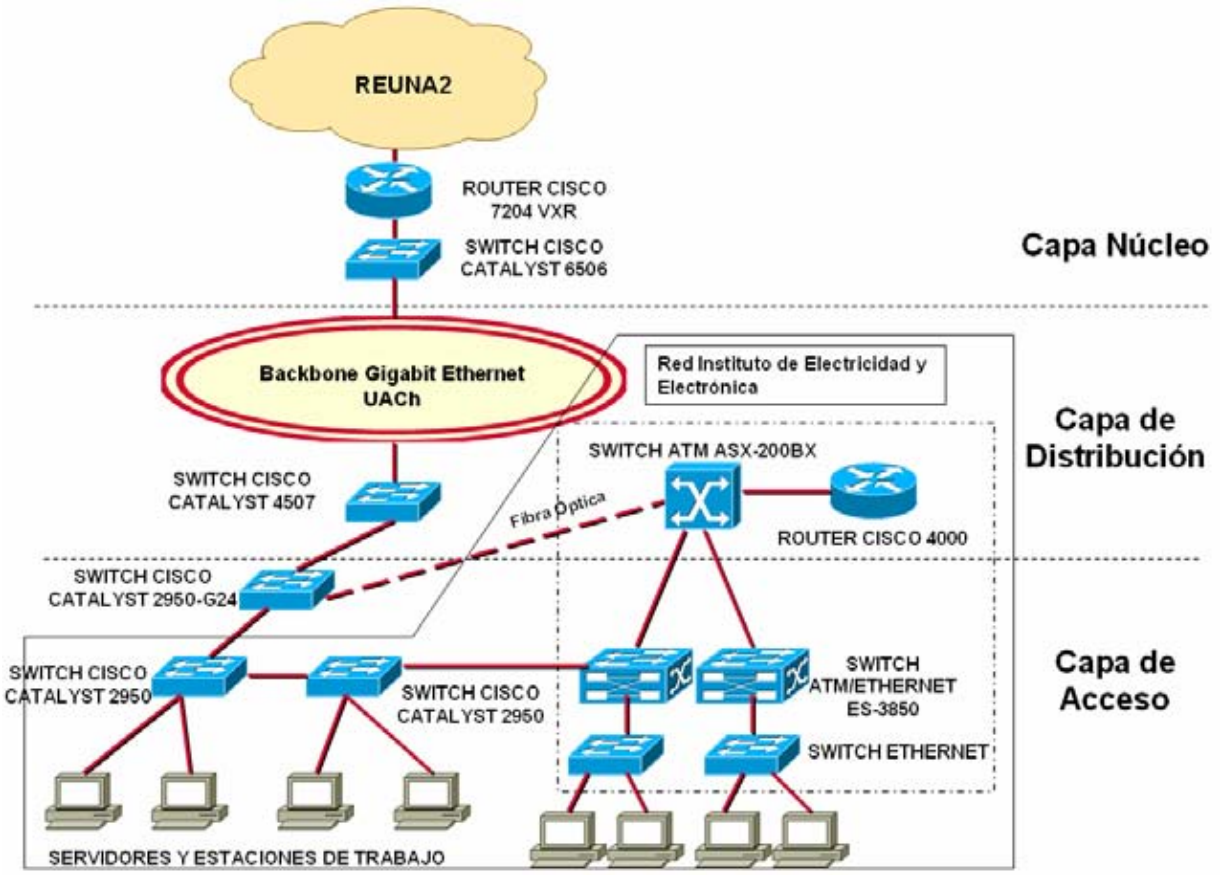

Fig. 3.1 – Propuesta de Red para el Instituto de Electricidad y Electrónica

En primera instancia esta tesis plantea instalar dos switch en el edificio de Ciencias Básicas, del Campus Miraflores, UACh. El primer switch Catalyst 2950-24 seria instalado en el segundo piso del edificio, este switch daría acceso a la red UACh e Internet a los académicos. El segundo switch, de similares características, estaría albergado en el Laboratorio de Redes y Conectividad y proveería de conexión a la red UACh y Internet a los servidores del laboratorio. Toda esta infraestructura descrita constituye la base para poder instalar una red de transporte de datos ATM, la que serviría como red paralela a la actual, pero dedicada exclusivamente al desarrollo de la investigación, crecimiento académico y mejoramiento del aprendizaje por intermedio de la experiencia practica. En este contexto, la necesidad de implementar esta nueva red con tecnología ATM, se debe principalmente al continuo avance de de la tecnología y la globalización que se experimenta hoy en día, que hace necesario que los futuros profesionales ingenieros formados en esta casa de estudios conozcan, experimenten y dominen la tecnología que hoy esta liderando el planeta.

3.3 PROPUESTA DE DIRECCIONAMIENTO LÓGICO

En segunda instancia, se deberán reasignar las direcciones IP y crear una política de direccionamiento con su correspondiente registro en el servidor DNS. Además, se creará la VLAN Lab_Redes de uso exclusivo por la red ATM registrada en el router principal.

En la siguiente tabla se plantea un esquema de direccionamiento lógico, el que identifica cada nodo conectado en la red:

- ***VLAN Ingeniería; Subred 200.2.114.0/24:***

Dirección IP	*Nombre de Host*	*Grupo de Trabajo*
Segmento Académicos		
200.2.114.200	direccion.elei.uach.cl	ELECTRONICA
200.2.114.201	secretaria.elei.uach.cl	ELECTRONICA
200.2.114.202	avillegas.elei.uach.cl	ELECTRONICA
200.2.114.203	rgutierrez.elei.uach.cl	ELECTRONICA
200.2.114.204	nfierro.elei.uach.cl	ELECTRONICA
200.2.114.205	cburgos.elei.uach.cl	ELECTRONICA
200.2.114.206	rreyes.elei.uach.cl	ELECTRONICA
200.2.114.207	jzarecht.elei.uach.cl	ELECTRONICA
200.2.114.208	fcastro.elei.uach.cl	ELECTRONICA
200.2.114.209	prey.elei.uach.cl	ELECTRONICA
Segmento Laboratorios		
200.2.114.210	reservado.elei.uach.cl	ELECTRONICA
200.2.114.211	reservado.elei.uach.cl	ELECTRONICA
200.2.114.212	reservado.elei.uach.cl	ELECTRONICA
200.2.114.213	reservado.elei.uach.cl	ELECTRONICA
200.2.114.214	reservado.elei.uach.cl	ELECTRONICA
Segmento Servidores		
200.2.114.215	senacitel.elei.uach.cl	ELECTRONICA
200.2.114.216	intranet.elei.uach.cl	ELECTRONICA
200.2.114.217	reservado.elei.uach.cl	ELECTRONICA

200.2.114.218	reservado.elei.uach.cl	ELECTRONICA
200.2.114.219	reservado.elei.uach.cl	ELECTRONICA
Segmento Reservado para Uso Futuro		
200.2.114.220	reservado.elei.uach.cl	ELECTRONICA
200.2.114.221	reservado.elei.uach.cl	ELECTRONICA
200.2.114.222	reservado.elei.uach.cl	ELECTRONICA
200.2.114.223	reservado.elei.uach.cl	ELECTRONICA
200.2.114.224	reservado.elei.uach.cl	ELECTRONICA
200.2.114.225	reservado.elei.uach.cl	ELECTRONICA

Tabla 3.1 – Propuesta de redireccionamiento VLAN Ingeniería

- ***VLAN Lab_Redes; Subred 172.16.96.0/24:***

Dirección IP	*Nombre de Host*
172.16.96.0	vlan-atm.labredes.elei.uach.cl
172.16.96.1	router-core.labredes.elei.uach.cl
172.16.96.2	router-cisco-4000.labredes.elei.uach.cl
172.16.96.3	atm-3850-1.labredes.elei.uach.cl
172.16.96.4	atm-3850-2.labredes.elei.uach.cl
172.16.96.5	atm-3850-3.labredes.elei.uach.cl
172.16.96.6	eth0-cisco-4000.labredes.elei.uach.cl
172.16.96.7	eth1-cisco-4000.labredes.elei.uach.cl
172.16.96.8	eth2-cisco-4000.labredes.elei.uach.cl
172.16.96.9	eth3-cisco-4000.labredes.elei.uach.cl
172.16.96.10 al 172.16.96.19	Reservado Servidores
172.16.96.20 al 172.16.249	Uso libre Académicos, Laboratorios y Alumnos.
172.16.96.252	asx-200.labredes.elei.uach.cl
172.16.96.253	reservado.labredes.elei.uach.cl
172.16.96.254	reservado.labredes.elei.uach.cl

Tabla 3.2 – Propuesta de redireccionamiento VLAN Lab_Redes

3.4 CABLEADO DE LA LAN

3.4.1 Generalidades

La presente memoria se refiere al sistema de cableado de datos a instalar en las oficinas del segundo piso del edificio 6000 de la Facultad de Ciencias de la Ingeniería de la Universidad Austral de Chile.

El cableado se implementará en base a un sistema de cableado estructurado, el cual será realizado con cable UTP categoría 5e.

3.4.2 Configuración

Cada puesto de trabajo salvo indicación contraria tendrá un conector RJ-45, de 8 contactos. Se instalará un rack para todo el cableado, el cual estará ubicado en el cuarto de centralización de 2º y un segundo rack en el Laboratorio de Redes y Conectividad para el cableado del laboratorio.

3.4.3 Alcance

El total de puestos a implementar es de:

- 15 puestos terminales para datos

Todos los elementos de conectividad serán preferentemente de una misma marca. El sistema se deberá entregar completo, probado y en correctas condiciones de funcionamiento.

3.4.4 Reglamentaciones y Normas

Se aplicarán las normas y reglamentos vigentes en la materia. (Anexo A.4)

3.4.5 Características del Cableado

Todo el Cableado de Datos a los puestos de trabajo será de acuerdo a las normas citadas, del tipo UTP categoría 5. Para Datos: Debe incluir todos los elementos del “Channel”, incluyendo “Patch Cord” al Switch y “Patch Cord” al Puesto de Trabajo (de 3 m de longitud) y conectores hembra RJ-45 (los conectores hembra RJ-45 deberán ser compatibles con las cajas de salida y plaquetas propuestas en cada caso).

El cableado asignado a Datos deberá soportar puestos de trabajo 100Base-TX.

Todo el cableado a los puestos de trabajo (Datos) será en cable UTP categoría 5, del tipo no propagador de llama.

Se deberán rotular con identificadores todas las llegadas o salidas en el rack, según se prevé en la norma EIA/TIA 606, entregándose las bases de datos de documentación tanto impresa como en soporte magnético. Cada conector RJ-45 en los puestos de trabajo tendrá la identificación correspondiente a su posición en el rack.

Se deberá especificar la marca y modelo de cada uno de los componentes de la instalación (los cuales deberán ser de marcas reconocidas), prefiriéndose componentes del “Channel” de una misma marca.

3.4.6 Patch Panel

Se instalarán en un Rack de 19” con capacidad para 24 unidades.

La conexión posterior de los patch panels se hará por medio de borneras tipo 110, “Krone” o similar. La conexión frontal se hará por medio de conectores tipo RJ-45, realizándose las mismas por cables UTP 5 con dos conectores “machos” de un metro de longitud.

CONCLUSIONES

Con el desarrollo de este trabajo ha quedado de manifiesto que Ethernet es una tecnología de gran flexibilidad, también que ha evolucionado rápidamente de una tecnología local a una de área metropolitana, incluso extensa y que hoy domina el mundo ofreciendo conectividad alámbrica con gran ancho de banda.

El uso de modelos de referencia divididos en capas facilita el entendimiento de la comunicación entre dos computadores en una red y proporcionar de una gran ayuda a la detección y solución de problemas.

La implementación de redes conmutadas permite un mayor aprovechamiento del ancho de banda disponible en una red, permitiendo crear pequeños dominios los que disminuyen el tráfico de broadcast.

Clasificar el diseño de una red en niveles jerárquicos, como la propuesta en este trabajo de tesis, permite seleccionar el hardware apropiado para cada nivel que se traduce en eficiencia y por consiguiente un aumento del rendimiento de la red, por lo tanto disminuyen los costos y tiempo de implementación.

La propuesta de mejoramiento de la red del Instituto de Electricidad y Electrónica, presentada en el capitulo 3 del presente trabajo, recomienda en primera instancia reemplazar los dispositivos concentradores de capa 1 (Hubs) existentes por dispositivos de capa 2 (Switches), transformándose de esta manera la red en una red conmutada, con lo que se obtendrá un mayor aprovechamiento del ancho de banda disponible. Para tener funcionalidades como calidad de servicio (QoS), administración remota, seguridad y/o creación de redes virtuales, la elección del hardware debe poseer la misma tecnología existente en la Red UACh.

En segunda instancia, junto con la instalación de los equipos de la nueva red ATM en el Laboratorio de Redes y Conectividad, es necesario instalar una línea de fibra óptica para interconectar el laboratorio al backbone Gigabit Ethernet UACh, creándose de esta manera una red alternativa y paralela a la red conmutada antes mencionada, sobre la cual se podrán realizar pruebas y mediciones de trafico con fines experimentales.

Una tercera recomendación es la creación de redes virtuales VLAN exclusivas para el desarrollo de experiencias de laboratorio controlando de esta manera el tráfico de broadcast de capa 3. La creación de VLAN desencadena un cambio en el direccionamiento de capa 3 en los nodos conectados a la red, el que puede ser con direcciones IP privadas y que por medio de NAT adquieren los mismos beneficios de conectividad que una dirección IP pública. Este redireccionamiento permite liberar direcciones IP públicas en uso y reservar su uso para aplicaciones.

Finalmente, la implementación de una red LAN para el Instituto de Electricidad y Electrónica de la Universidad Austral de Chile, constituye una poderosa herramienta para el desarrollo de la investigación y también un apoyo en las actividades académicas de los estudiantes, pues permitirá que los alumnos puedan experimentar con equipos y conocer la tecnología con la que trabajaran, cuando ingresen al mundo laboral.

BIBLIOGRAFÍA

[CISCO2004] **"Cisco Networking Academy Program CCNA 1-4 Course"**, Cisco Systems, Inc., 2004.

[GONZA2005] González Kaempfer, Héctor Osvaldo, **"Laboratorio de Redes de Datos"**, Universidad Austral de Chile, Valdivia, 2005.

[OPPEN2004] Oppenheimer, Priscilla, **"Top-Down Network Design"**, Second Edition, Cisco Press, Indianapolis, USA, 2004.

[PELLO2005] **"IPTABLES Manual Práctico"**, Pello Xavier Altadill Izura, http://www.pello.info/ - 16/07/2005, 13:00.

[TANEN1997] Tanenbaum, Andrew S., **"Redes de Computadoras"**, Tercera Edición, Prentice Hall, México, 1997.

[TRADU2005] **"Traducción de Direcciones de Red (NAT)"**, http://www.openbsd.org/faq/pf/es/nat.html, 19/07/2005, 16:50.

ANEXOS

A.1 DIRECCIONAMIENTO IP

Para que dos sistemas se comuniquen, se deben poder identificar y localizar entre sí. Cada computador conectado a una red TCP/IP debe recibir un identificador exclusivo o una dirección IP. Esta dirección, que opera en la Capa 3, permite que un computador localice otro computador en la red. Todos los computadores también cuentan con una dirección física exclusiva, conocida como dirección MAC. Estas son asignadas por el fabricante de la tarjeta de interfaz de la red. Las direcciones MAC operan en la Capa 2 del modelo OSI.

Una dirección IP es una secuencia de unos y ceros de 32 bits. Para que el uso de la dirección IP sea más sencillo, en general, la dirección aparece escrita en forma de cuatro números decimales separados por puntos. Por ejemplo, la dirección IP de un computador es 192.168.1.2. Esta forma de escribir una dirección se conoce como formato decimal punteado. En esta notación, cada dirección IP se escribe en cuatro partes separadas por puntos. Cada parte de la dirección se conoce como octeto porque se compone de ocho dígitos binarios. La notación decimal punteada es un método más sencillo de comprender que el método binario de unos y ceros. Esta notación decimal punteada también evita que se produzca una gran cantidad de errores por transposición, que sí se produciría si sólo se utilizaran números binarios. El uso de decimales separados por puntos permite una mejor comprensión de los patrones numéricos.

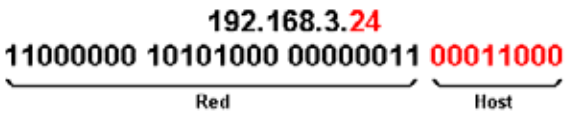

Fig. A.1 – Dirección IP

A.1.1 Direcciones IP Clase A, B, C, D y E

Para adaptarse a redes de distintos tamaños y para ayudar a clasificarlas, las direcciones IP se dividen en grupos llamados clases. Esto se conoce como direccionamiento classful. Cada dirección IP completa de 32 bits se divide en la parte de la red y parte del host. Un bit o una secuencia de bits al inicio de cada dirección determinan su clase. Son cinco las clases de direcciones IP.

Clase A	Red	Host		
Octet	1	2	3	4

Clase B	Red		Host	
Octet	1	2	3	4

Clase C	Red			Host
Octet	1	2	3	4

Clase D	Host			
Octet	1	2	3	4

Fig. A.2 – Prefijo de clases de dirección

La dirección Clase A se diseñó para admitir redes de tamaño extremadamente grande, de más de 16 millones de direcciones de host disponibles. Las direcciones IP Clase A utilizan sólo el primer octeto para indicar la dirección de la red. Los tres octetos restantes son para las direcciones host.

El primer bit de la dirección Clase A siempre es 0. Con dicho primer bit, que es un 0, el menor número que se puede representar es 00000000, 0 decimal. El valor más alto que se puede representar es 01111111, 127 decimal. Estos números 0 y 127 quedan reservados y no se pueden utilizar como direcciones de red. Cualquier dirección que comience con un valor entre 1 y 126 en el primer octeto es una dirección Clase A.

La red 127.0.0.0 se reserva para las pruebas de loopback. Los Routers o las máquinas locales pueden utilizar esta dirección para enviar paquetes nuevamente hacia ellos mismos. Por lo tanto, no se puede asignar este número a una red.

La dirección Clase B se diseñó para cumplir las necesidades de redes de tamaño moderado a grande. Una dirección IP Clase B utiliza los primeros dos de los cuatro octetos para indicar la dirección de la red. Los dos octetos restantes especifican las direcciones del host.

Los primeros dos bits del primer octeto de la dirección Clase B siempre son 10. Los seis bits restantes pueden poblarse con unos o ceros. Por lo tanto, el menor número que puede representarse en una dirección Clase B es 10000000, 128 decimal. El número más alto que

puede representarse es 10111111, 191 decimal. Cualquier dirección que comience con un valor entre 128 y 191 en el primer octeto es una dirección Clase B.

El espacio de direccionamiento Clase C es el que se utiliza más frecuentemente en las clases de direcciones originales. Este espacio de direccionamiento tiene el propósito de admitir redes pequeñas con un máximo de 254 hosts.

Una dirección Clase C comienza con el binario 110. Por lo tanto, el menor número que puede representarse es 11000000, 192 decimal. El número más alto que puede representarse es 11011111, 223 decimal. Si una dirección contiene un número entre 192 y 223 en el primer octeto, es una dirección de Clase C.

La dirección Clase D se creó para permitir multicast en una dirección IP. Una dirección multicast es una dirección exclusiva de red que dirige los paquetes con esa dirección destino hacia grupos predefinidos de direcciones IP. Por lo tanto, una sola estación puede transmitir de forma simultánea una sola corriente de datos a múltiples receptores.

El espacio de direccionamiento Clase D, en forma similar a otros espacios de direccionamiento, se encuentra limitado matemáticamente. Los primeros cuatro bits de una dirección Clase D deben ser 1110. Por lo tanto, el primer rango de octeto para las direcciones Clase D es 11100000 a 11101111, o 224 a 239. Una dirección IP que comienza con un valor entre 224 y 239 en el primer octeto es una dirección Clase D.

Se ha definido una dirección Clase E. Sin embargo, la Fuerza de Tareas de Ingeniería de Internet (IETF) ha reservado estas direcciones para su propia investigación. Por lo tanto, no se han emitido direcciones Clase E para ser utilizadas en Internet. Los primeros cuatro bits de una dirección Clase E siempre son 1s. Por lo tanto, el rango del primer octeto para las direcciones Clase E es 11110000 a 11111111, o 240 a 255.

La Figura A.3 muestra el rango de las direcciones IP del primer octeto tanto en decimales como en binarios para cada clase de dirección IP.

Clase de dirección IP	Intervalo de dirección IP (Valor decimal d
Clase A	1-126 (00000001-01111110) *
Clase B	128-191 (10000000-10111111)
Clase C	192-223 (11000000-11011111)
Clase D	224-239 (11100000-11101111)
Clase E	240-255 (11110000-11111111)

Fig. A.3 – Intervalo de dirección IP

A.1.2 Direcciones IP Reservadas

Ciertas direcciones de host son reservadas y no pueden asignarse a dispositivos de la red. Estas direcciones de host reservadas incluyen:

- **Dirección de red:** Utilizada para identificar la red en sí.
- **Dirección de broadcast:** Utilizada para realizar el broadcast de paquetes hacia todos los dispositivos de una red.

La dirección IP que tiene ceros binarios en todas las posiciones de bits de host, queda reservada para la dirección de red. Tomando como ejemplo una red Clase A,113.0.0.0 es la dirección IP de la red, conocida como el ID (identificador) de la red, que contiene el host 113.1.2.3. Un Router usa la dirección IP de red al enviar datos por Internet.

Para enviar información a todos los dispositivos de la red, se necesita una dirección de broadcast. Un broadcast se produce cuando una fuente envía datos a todos los dispositivos de una red. Para asegurar que todos los demás dispositivos de una red procesen el broadcast, el transmisor debe utilizar una dirección IP destino que ellos puedan reconocer y procesar. Las direcciones IP de broadcast terminan con unos binarios en toda la parte de la dirección que corresponde al host.

A.1.3 Direcciones IP Públicas y Privadas

La estabilidad de la Internet depende de forma directa de la exclusividad de las direcciones de red utilizadas públicamente.

Las direcciones IP públicas son exclusivas. Dos máquinas que se conectan a una red pública nunca pueden tener la misma dirección IP porque las direcciones IP públicas son globales y están estandarizadas. Todas las máquinas que se conectan a la Internet acuerdan adaptarse al sistema. Hay que obtener las direcciones IP públicas de un proveedor de servicios de Internet (ISP) o un registro, a un costo.

Con el rápido crecimiento de Internet, las direcciones IP públicas comenzaron a escasear. Se desarrollaron nuevos esquemas de direccionamiento, tales como el enrutamiento entre dominios sin clase (CIDR) y el IPv6, para ayudar a resolver este problema.

Las direcciones IP privadas son otra solución al problema del inminente agotamiento de las direcciones IP públicas. Como ya se ha mencionado, las redes públicas requieren que los hosts tengan direcciones IP únicas. Sin embargo, las redes privadas que no están conectadas a la Internet pueden utilizar cualquier dirección de host, siempre que cada host dentro de la red privada sea exclusivo. Existen muchas redes privadas junto con las redes públicas. Sin embargo, no es recomendable que una red privada utilice una dirección cualquiera debido a que, con el tiempo, dicha red podría conectarse a Internet. El RFC 1918 asigna tres bloques de la dirección IP para uso interno y privado. Estos tres bloques consisten en una dirección de Clase A, un rango de direcciones de Clase B y un rango de direcciones de Clase C. Las direcciones que se encuentran en estos rangos no se enrutan hacia el backbone de la Internet. Los Routers de Internet descartan inmediatamente las direcciones privadas. Si se produce un direccionamiento hacia una intranet que no es pública, un laboratorio de prueba o una red doméstica, es posible utilizar las direcciones privadas en lugar de direcciones exclusivas a nivel global. Las direcciones IP privadas pueden entremezclarse con las direcciones IP públicas. Así, se conservará el número de direcciones utilizadas para conexiones internas.

La conexión de una red que utiliza direcciones privadas a la Internet requiere que las direcciones privadas se conviertan a direcciones públicas. Este proceso de conversión se

conoce como Traducción de Direcciones de Red (NAT). En general, un Router es el dispositivo que realiza la NAT.

Clase	intervalo de direcciones internas RFC 1918
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

Fig. A.4 – Direcciones IP privadas

A.1.4 IPv4 e IPv6

Se ha definido y desarrollado una versión más extensible y escalable del IP, la Versión 6 del IP (IPv6). IPv6 utiliza 128 bits en lugar de los 32 bits que en la actualidad utiliza el IPv4. IPv6 utiliza números hexadecimales para representar los 128 bits. IPv6 proporciona 640 sextillones de direcciones. Esta versión del IP proporciona un número de direcciones suficientes para futuras necesidades de comunicación. Esta versión de IP debe proporcionar suficientes direcciones para las necesidades de comunicación futuras.

Las direcciones de IPv4 miden 32 bits de longitud, se escriben con números decimales separados por puntos. Las direcciones IPv6 miden 128 bits y son identificadores de interfaces individuales y conjuntos de interfaces. Las direcciones IPv6 se asignan a interfaces, no a nodos. Como cada interface pertenece a un solo nodo, cualquiera de las direcciones unicast asignada a las interfaces del nodo se pueden usar como identificadores del nodo. Las direcciones IPv6 se escriben en hexadecimal, separados por comas. Los campos IPv6 tienen una longitud de 16 bits. Para que las direcciones sean más fáciles de leer, es posible omitir los ceros iniciales de cada campo. El campo: 0003: se escribe :3:. La representación taquigráfica del IPv6 de los 128 bits utiliza números de 16 dígitos, que se muestran en forma de cuatro dígitos hexadecimales.

Después de diez años de planificación y desarrollo, el IPv6 lentamente comienza a implementarse en redes selectas. Con el tiempo, el IPv6 podrá reemplazar el IPv4 como el protocolo de Internet dominante.

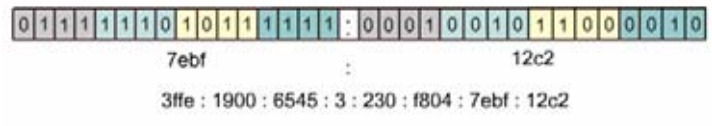

Fig. A.5 – Dirección IPv6

A.2 DISPOSITIVOS DE RED

A.2.1 Repetidores

El término repetidor proviene de los inicios de las comunicaciones de larga distancia. Un repetidor recibe una señal, la regenera, y la transmite. El propósito de un repetidor es regenerar y retemporizar las señales de red a nivel de los bits para permitir que los bits viajen a mayor distancia a través de los medios. En Ethernet e IEEE 802.3 se implementa la “regla 5-4-3”, en referencia al número de repetidores y segmentos en un Backbone de acceso compartido con topología de árbol. La “regla 5-4-3 divide la red en dos tipos de segmentos físicos: Segmentos Poblados (de usuarios), y Segmentos no Poblados (enlaces). En los segmentos poblados se conectan los sistemas de los usuarios. Los segmentos no poblados se usan para conectar los repetidores de la red entre si. La regla manda que entre cualquiera dos nodos de una red, puede existir un máximo de cinco segmentos, conectados por cuatro repetidores o concentradores, y solamente tres de los cinco segmentos pueden tener usuarios conectados a los mismos.

El protocolo Ethernet requiere que una señal enviada en la LAN alcance cualquier parte de la red dentro de una longitud de tiempo especificada. La “regla 5-4-3” asegura que esto pase. Cada repetidor a través del cual pasa la señal añade una pequeña cantidad de tiempo al proceso, por lo que la regla está diseñada para minimizar el tiempo de transmisión de la señal. Demasiada latencia en la LAN incrementa la cantidad de colisiones tardías, haciendo la LAN menos eficiente.

A.2.2 Hubs

Los hubs en realidad son repetidores multipuerto. En muchos casos, la diferencia entre los dos dispositivos radica en el número de puertos que cada uno posee. Mientras que un repetidor convencional tiene sólo dos puertos, un hub por lo general tiene de cuatro a veinticuatro puertos. Los hubs por lo general se utilizan en las redes Ethernet 10BASE-T o 100BASE-T, aunque hay otras arquitecturas de red que también los utilizan.

El uso de un hub hace que cambie la topología de la red desde un bus lineal, donde cada dispositivo se conecta de forma directa al cable, a una en estrella. En un hub, los datos que llegan a un puerto del hub se transmiten de forma eléctrica a todos los otros puertos conectados al mismo segmento de red, salvo a aquel puerto desde donde enviaron los datos.

Los hubs vienen en tres tipos básicos:

- **Pasivo:** Un hub pasivo sirve sólo como punto de conexión física. No manipula o visualiza el tráfico que lo cruza. No amplifica o limpia la señal. Un hub pasivo se utiliza sólo para compartir los medios físicos. En sí, un hub pasivo no requiere energía eléctrica.
- **Activo:** Se debe conectar un hub activo a un tomacorriente porque necesita alimentación para amplificar la señal entrante antes de pasarla a los otros puertos.
- **Inteligente:** A los hubs inteligentes a veces se los denomina "smart hubs". Estos dispositivos básicamente funcionan como hubs activos, pero también incluyen un chip microprocesador y capacidades diagnósticas. Los hubs inteligentes son más costosos que los hubs activos, pero resultan muy útiles en el diagnóstico de fallas.

Los dispositivos conectados al hub reciben todo el tráfico que se transporta a través del hub. Cuántos más dispositivos están conectados al hub, mayores son las probabilidades de que haya colisiones. Las colisiones ocurren cuando dos o más estaciones de trabajo envían al mismo tiempo datos a través del cable de la red. Cuando esto ocurre, todos los datos se corrompen. Cada dispositivo conectado al mismo segmento de red se considera un miembro de un dominio de colisión.

Algunas veces los hubs se llaman concentradores, porque los hubs sirven como punto de conexión central para una LAN de Ethernet

A.2.3 Puentes

A veces, es necesario dividir una LAN grande en segmentos más pequeños que sean más fáciles de manejar. Esto disminuye la cantidad de tráfico en una sola LAN y puede extender el área geográfica más allá de lo que una sola LAN puede admitir. Los dispositivos que se usan para conectar segmentos de redes son los puentes, switches, routers y gateways. Los switches y los puentes operan en la capa de enlace de datos del modelo de referencia OSI. La función del puente es tomar decisiones inteligentes con respecto a pasar señales o no al segmento siguiente de la red.

Cuando un puente recibe una trama a través de la red, se busca la dirección MAC destino en la tabla de puenteo para determinar si hay que filtrar, inundar, o copiar la trama en otro segmento. El proceso de decisión tiene lugar de la siguiente forma:

- Si el dispositivo destino se encuentra en el mismo segmento que la trama, el puente impide que la trama vaya a otros segmentos. Este proceso se conoce como filtrado.
- Si el dispositivo destino está en un segmento distinto, el puente envía la trama hasta el segmento apropiado.
- Si el puente desconoce la dirección destino, el puente envía la trama a todos los segmentos excepto aquel en el cual se recibió. Este proceso se conoce como inundación.
- Si se ubica de forma estratégica, un puente puede mejorar el rendimiento de la red de manera notoria

A.2.4 Switches

Un switch se describe a veces como un puente multipuerto. Mientras que un puente típico puede tener sólo dos puertos que enlacen dos segmentos de red, el switch puede tener varios puertos, según la cantidad de segmentos de red que sea necesario conectar. Al igual que los puentes, los switches aprenden determinada información sobre los paquetes de datos que

se reciben de los distintos computadores de la red. Los switches utilizan esa información para crear tablas de envío para determinar el destino de los datos que se están mandando de un computador a otro de la red.

Aunque hay algunas similitudes entre los dos, un switch es un dispositivo más sofisticado que un puente. Un puente determina si se debe enviar una trama al otro segmento de red, basándose en la dirección MAC destino. Un switch tiene muchos puertos con muchos segmentos de red conectados a ellos. El switch elige el puerto al cual el dispositivo o estación de trabajo destino está conectado. Los switches Ethernet están llegando a ser soluciones para conectividad de uso difundido porque, al igual que los puentes, los switches mejoran el rendimiento de la red al mejorar la velocidad y el ancho de banda.

La conmutación es una tecnología que alivia la congestión en las LAN Ethernet, reduciendo el tráfico y aumentando el ancho de banda. Los switches pueden remplazar a los hubs con facilidad debido a que ellos funcionan con las infraestructuras de cableado existentes. Esto mejora el rendimiento con un mínimo de intrusión en la red ya existente.

Actualmente en la comunicación de datos, todos los equipos de conmutación realizan dos operaciones básicas: La primera operación se llama conmutación de las tramas de datos. La conmutación de las tramas de datos es el procedimiento mediante el cual una trama se recibe en un medio de entrada y luego se transmite a un medio de salida. El segundo es el mantenimiento de operaciones de conmutación cuando los switch crean y mantienen tablas de conmutación y buscan loops.

Los switches operan a velocidades mucho más altas que los puentes y pueden admitir nuevas funcionalidades como, por ejemplo, las LAN virtuales.

Un switch Ethernet ofrece muchas ventajas. Un beneficio es que un switch para Ethernet permite que varios usuarios puedan comunicarse en paralelo usando circuitos virtuales y segmentos de red dedicados en un entorno virtualmente sin colisiones. Esto aumenta al máximo el ancho de banda disponible en el medio compartido. Otra de las ventajas es que desplazarse a un entorno de LAN conmutado es muy económico ya que el hardware y el cableado se pueden volver a utilizar

A.2.5 Router

Un router es un tipo especial de computador. Cuenta con los mismos componentes básicos que un PC estándar de escritorio. Cuenta con una CPU, memoria, bus de sistema y distintas interfaces de entrada/salida. Sin embargo, los routers están diseñados para cumplir algunas funciones muy específicas que, en general, no realizan los computadores de escritorio.

Aunque se pueda usar un router para segmentar las LAN, su uso fundamental es como dispositivo WAN. Los routers tienen interfaces LAN y WAN. De hecho, los routers se comunican entre sí por medio de conexiones WAN. Los routers son la columna vertebral de las grandes redes internas y de Internet. Operan en la capa 3 del modelo OSI, tomando decisiones basadas en las direcciones de red. Las dos principales funciones de un router son la selección de la mejor ruta para y la conmutación de las tramas hacia la interfaz correspondiente. Los routers logran esto por medio de la creación de tablas de enrutamiento y el intercambio de información de red de estas tablas con otros routers.

A.3 REDES INALÁMBRICAS

A.3.1 Estándares y Organizaciones del las LAN Inalámbricas

Como en el caso de las redes cableadas, la IEEE es la principal generadora de estándares para las redes inalámbricas. Los estándares han sido creados en el marco de las reglamentaciones creadas por el Comité Federal de Comunicaciones (Federal Communications Commission - FCC).

La tecnología clave que contiene el estándar 802.11 es el Espectro de Dispersión de Secuencia Directa (DSSS). El DSSS se aplica a los dispositivos inalámbricos que operan dentro de un intervalo de 1 a 2 Mbps. Un sistema de DSSS puede transmitir hasta 11 Mbps, pero si opera por encima de los 2 Mbps se considera que no cumple con la norma. El siguiente estándar aprobado fue el 802.11b, que aumentó las capacidades de transmisión a 11 Mbps. Aunque las WLAN de DSSS podían interoperar con las WLAN de Espectro de Dispersión por Salto de Frecuencia (FHSS), se presentaron problemas que motivaron a los fabricantes a

realizar cambios en el diseño. En este caso, la tarea del IEEE fue simplemente crear un estándar que coincidiera con la solución del fabricante.

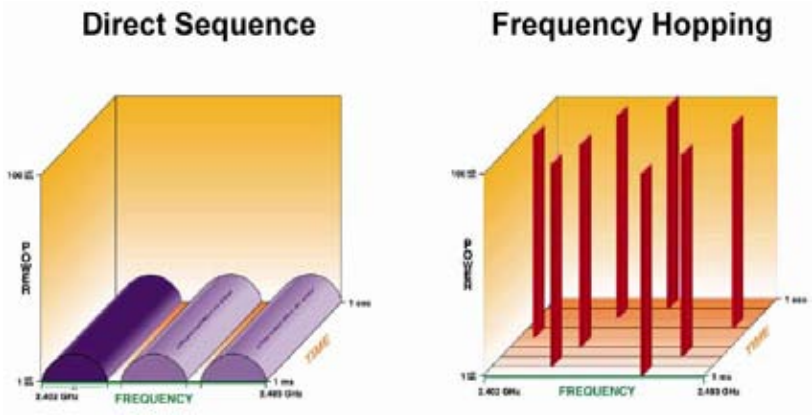

Fig. A.6 – Tecnologías DSSS y FHSS

802.11b también recibe el nombre de Wi-Fi™ o inalámbrico de alta velocidad y se refiere a los sistemas DSSS que operan a 1, 2; 5,5 y 11 Mbps. Todos los sistemas 802.11b cumplen con la norma de forma retrospectiva, ya que también son compatibles con 802.11 para velocidades de transmisión de datos de 1 y 2 Mbps sólo para DSSS. Esta compatibilidad retrospectiva es de suma importancia ya que permite la actualización de la red inalámbrica sin reemplazar las NIC o los puntos de acceso.

Los dispositivos de 802.11b logran un mayor índice de tasa de transferencia de datos ya que utilizan una técnica de codificación diferente a la del 802.11, permitiendo la transferencia de una mayor cantidad de datos en la misma cantidad de tiempo. La mayoría de los dispositivos 802.11b todavía no alcanzan tasa de transferencia de 11 Mbps y, por lo general, trabajan en un intervalo de 2 a 4 Mbps.

802.11a abarca los dispositivos WLAN que operan en la banda de transmisión de 5 GHZ. El uso del rango de 5 GHZ no permite la interoperabilidad de los dispositivos 802.11b ya que éstos operan dentro de los 2,4 GHZ. 802.11a puede proporcionar una tasa de transferencia de datos de 54 Mbps y con una tecnología propietaria que se conoce como "duplicación de la velocidad" ha alcanzado los 108 Mbps. En las redes de producción, la velocidad estándar es de 20-26 Mbps.

802.11g ofrece tasa de transferencia que 802.11a pero con compatibilidad retrospectiva para los dispositivos 802.11b utilizando tecnología de modulación por Multiplexión por División de Frecuencia Ortogonal (OFDM).

A.3.2 Dispositivos y Topologías Inalámbricas

Una red inalámbrica puede constar de tan sólo dos dispositivos. Los nodos pueden ser simples estaciones de trabajo de escritorio o computadores de mano. Equipada con NIC inalámbricas, se puede establecer una red Ad-Hoc comparable a una red cableada de par a par. Ambos dispositivos funcionan como servidores y clientes en este entorno. Aunque brinda conectividad, la seguridad es mínima, al igual que la tasa de transferencia. Otro problema de este tipo de red es la compatibilidad. Muchas veces, las NIC de diferentes fabricantes no son compatibles.

Para resolver el problema de la compatibilidad, se suele instalar un punto de acceso (AP) para que actúe como hub central para el modo de infraestructura de la WLAN. El AP se conecta mediante cableado a la LAN cableada a fin de proporcionar acceso a Internet y conectividad a la red cableada. Los AP están equipados con antenas y brindan conectividad inalámbrica a un área específica que recibe el nombre de celda. Según la composición estructural del lugar donde se instaló el AP y del tamaño y ganancia de las antenas, el tamaño de la celda puede variar enormemente. Por lo general, el alcance es de 91,44 a 152,4 metros (300 a 500 pies). Para brindar servicio a áreas más extensas, es posible instalar múltiples puntos de acceso con cierto grado de superposición. Esta superposición permite pasar de una celda a otra (roaming). Esto es muy parecido a los servicios que brindan las empresas de teléfonos celulares. La superposición, en redes con múltiples puntos de acceso, es fundamental para permitir el movimiento de los dispositivos dentro de la WLAN. Aunque los estándares del IEEE no determinan nada al respecto, es aconsejable una superposición de un 20-30% . Este índice de superposición permitirá el roaming entre las celdas y así la actividad de desconexión y reconexión no tendrá interrupciones.

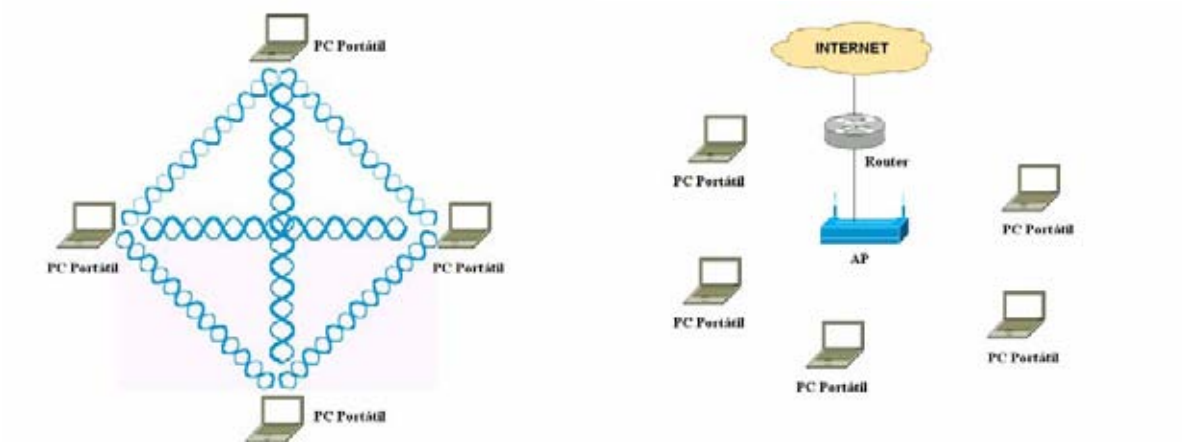

Fig. A.7 – Topologías Ad-Hoc e Infraestructura

Cuando se activa un cliente dentro de la WLAN, la red comenzará a "escuchar" para ver si hay un dispositivo compatible con el cual "asociarse". Esto se conoce como "escaneo" y puede ser activo o pasivo.

El escaneo activo hace que se envíe un pedido de sondeo desde el nodo inalámbrico que busca conectarse a la red. Este pedido de sondeo incluirá el Identificador del Servicio (SSID) de la red a la que se desea conectar. Cuando se encuentra un AP con el mismo SSID, el AP emite una respuesta de sondeo. Se completan los pasos de autenticación y asociación.

Los nodos de escaneo pasivo esperan las tramas de administración de beacons (beacons) que son transmitidas por el AP (modo de infraestructura) o nodos pares (ad hoc). Cuando un nodo recibe un beacon que contiene el SSID de la red a la que se está tratando de conectar, se realiza un intento de conexión a la red. El escaneo pasivo es un proceso continuo y los nodos pueden asociarse o desasociarse de los AP con los cambios en la potencia de la señal.

A.3.3 Cómo se Comunican las LAN Inalámbricas

Una vez establecida la conectividad con la WLAN, un nodo pasará las tramas de igual forma que en cualquier otra red 802.x. Las WLAN no usan una trama estándar 802.3. Por lo tanto, el término "Ethernet Inalámbrica" puede resultar engañoso. Hay tres clases de tramas: de control, de administración y de datos. Sólo la trama de datos es parecida las tramas 802.3. Las

tramas inalámbricas y la 802.3 cargan 1500 bytes; sin embargo una trama de Ethernet no puede superar los 1518 bytes mientras que una trama inalámbrica puede alcanzar los 2346 bytes. En general, el tamaño de la trama de WLAN se limita a 1518 bytes ya que se conecta, con mayor frecuencia, a una red cableada de Ethernet.

Debido a que la radiofrecuencia (RF) es un medio compartido, se pueden producir colisiones de la misma manera que se producen en un medio compartido cableado. La principal diferencia es que no existe un método por el que un nodo origen pueda detectar que ha ocurrido una colisión. Por eso, las WLAN utilizan Acceso Múltiple con Detección de Portadora y Prevención de Colisiones (CSMA/CA). Es parecido al CSMA/CD de Ethernet.

Cuando un nodo fuente envía una trama, el nodo receptor devuelve un acuse de recibo positivo (ACK). Esto puede consumir un 50% del ancho de banda disponible. Este gasto, al combinarse con el del protocolo de prevención de colisiones reduce la tasa de transferencia real de datos a un máximo de 5,0 a 5,5 Mbps en una LAN inalámbrica 802.11b con una velocidad de 11 Mbps.

El rendimiento de la red también estará afectado por la potencia de la señal y por la degradación de la calidad de la señal debido a la distancia o interferencia. A medida que la señal se debilita, se puede invocar la Selección de Velocidad Adaptable (ARS). La unidad transmisora disminuirá la velocidad de transmisión de datos de 11 Mbps a 5,5 Mbps, de 5,5 Mbps a 2 Mbps o de 2 Mbps a 1 Mbps.

A.4 CABLEADO ESTRUCTURADO

A.4.1 Especificaciones de Instalación

Para un buen diseño e implementación de Cableado Estructurado, es necesario tener en cuenta los siguientes subsistemas:

- Cableado Horizontal
- Cableado Vertical (Backbone)
- Cuarto de Telecomunicaciones
- Cuarto de Equipos
- Cuarto de Entrada de Servicios

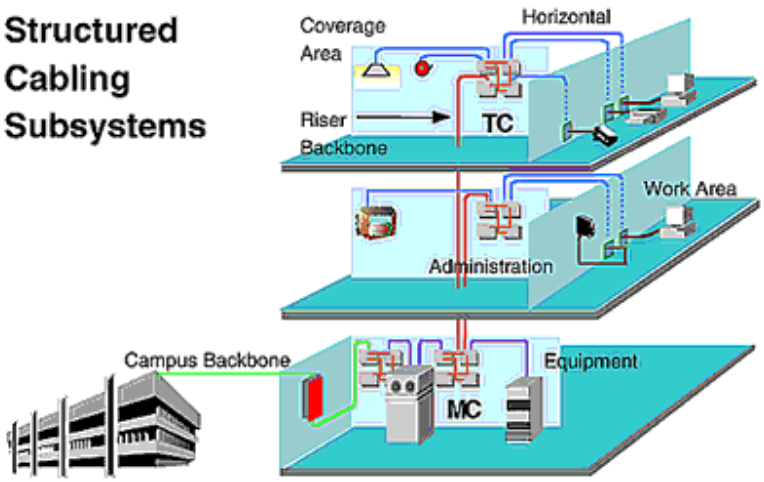

Fig. A.8 – Sistema de Cableado Estructurado

A.4.1.1 Cableado Horizontal

El cableado horizontal es la porción del sistema de cableado que se extiende desde el closet de telecomunicaciones (Rack) hasta el usuario final en su estación de trabajo y consta de:

I. Cable Horizontal y Hardware de Conexión. (cableado horizontal)
II. Rutas y Espacios Horizontales. (sistemas de distribución horizontal)

El término horizontal es utilizado debido a que típicamente el sistema de cableado se instala horizontalmente a través del piso o del techo del edificio. El cableado horizontal consta de cable par trenzado de cobre, aunque si se requiere un alto rendimiento se puede utilizar fibra óptica. El cableado horizontal se debe implementar en una topología de estrella. Cada punto terminal de conexión de Datos y/o Voz debe estar conectado al Patch Panel.

A.4.1.1.1 Consideraciones para el cableado horizontal:

1. Distancias Horizontales

La máxima distancia horizontal permitida es de 90 metros (295 ft) independiente del tipo de medio. Esta es la distancia máxima entre el Patch Panel y el Terminal de conexión. La longitud máxima del punto terminal hasta la estación de trabajo es de 3 metros (9.8 ft).

2.Tipos de Cables

Existen tres tipos de cables que pueden ser utilizados en los sistemas de cableado horizontal:

- Cable UTP (Unshielded Twisted Pair) de 4 pares a 100 W.
- Cable STP (Shielded Twisted Pair) de 2 pares a 150 W.
- Fibra Optica 62.5/125 mm de 2 pares.

El cable a utilizar por excelencia es el par trenzado sin blindaje UTP de cuatro pares categoría 5. El cable coaxial de 50 ohmios se acepta pero no se recomienda en instalaciones nuevas.

3. Salidas de Área de Trabajo

Los ductos a las salidas de área de trabajo (work area outlet, WAO) deben preveer la capacidad de manejar tres cables. Las salidas de área de trabajo deben contar con un mínimo

de dos conectores. Uno de los conectores debe ser del tipo RJ-45 bajo el código de colores de cableado T568A (recomendado) o T568B.

A.4.1.2 Cableado Vertical (Backbone)

El Backbone provee interconexión entre el cuarto de telecomunicaciones, cuarto de equipos y la entrada al edificio. Este consiste del cable Backbone, del cross-connect intermedio y principal, de las terminaciones mecánicas y de los patch cords. El Rack, el cuarto de equipos y los puntos demarcados pueden estar localizados en diferentes edificios; el Backbone incluye los medio de transmisión entre diferentes edificios. El cableado vertical debe soportar todos los dispositivos que están dentro del Rack y a menudo todas las impresoras, terminales y servidores de archivo de un piso de un edificio. El cableado vertical se presenta en diferentes topologías, la más usada es la topología en estrella.

A.4.1.3 Cuarto de Telecomunicaciones

Un cuarto de telecomunicaciones es el área en un edificio utilizada para el uso exclusivo de equipo asociado con el sistema de cableado de telecomunicaciones. El espacio del cuarto de comunicaciones no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones. El cuarto de telecomunicaciones debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado. El diseño de cuartos de telecomunicaciones debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad, audio y otros sistemas de telecomunicaciones. Todo edificio debe contar con al menos un cuarto de telecomunicaciones o cuarto de equipo. No hay un límite máximo en la cantidad de cuartos de telecomunicaciones que puedan haber en un edificio.

A.4.1.4 Cuarto de Equipos

El cuarto de equipos es un espacio centralizado para los equipos de telecomunicaciones (Ej. PBX, Equipos de Cómputo, Switch), que sirven a los ocupantes del edificio. Este cuarto, únicamente debe guardar equipos directamente relacionados con el sistema de

telecomunicaciones y sus sistemas de soporte. La norma que estandariza este subsistema es la EIA/TIA 569.

A.4.1.5 Cuarto de Entrada de Servicios

La entrada de servicios provee el punto en el cual el cableado externo se une con el cableado vertical (backbone) interno del edificio. Los requerimientos físicos de dicha interfase están definidos en la norma EIA/TIA 569. Este consiste en una entrada de servicios de telecomunicaciones al edificio, la cual incluye el punto de entrada a través de la pared del edificio y continuando al cuarto o área de entrada. La entrada al edificio debe contener la ruta del backbone que interconecta con los otros edificios del campus. En caso de una comunicación a través de una antena, esta también pertenece a la Entrada al Edificio.

A.4.1.6 Requerimientos de Funcionamiento y de Ancho de Banda.

Los diferentes sistemas de cableado ofrecen distintas características de funcionamiento. La variedad de velocidad de transmisión de los datos que un sistema de cableado puede acomodar, se conoce como el ancho de banda utilizable. La capacidad del ancho de banda está dictada por las características de comportamiento eléctrico que los componentes del sistema de cableado tengan. Ésto viene a ser especialmente importante cuando se están planeando futuras aplicaciones que impondrán mayores demandas sobre el sistema de cableado. El funcionamiento del sistema de cableado deberá ser considerado no sólo cuando se está apoyando las necesidades actuales sino también cuando se anticipan las necesidades del mañana. Hacer ésto permitirá la migración a aplicaciones de redes más rápidas sin necesidad de incurrir en costosas actualizaciones del sistema de cableado.

A.4.1.7 Recomendaciones en Cuanto a Canalizaciones y Ductos

- Los cables UTP no deben circular junto a cables de energía dentro de la misma cañería por más corto que sea el trayecto.
- Debe evitarse el cruce de cables UTP con cables de energía. De ser necesario, estos deben realizarse a 90°.

- Los cables UTP pueden circular por bandeja compartida con cables de energía respetando el paralelismo a una distancia mínima de 10 cm. En el caso de existir una división metálica puesta a tierra, esta distancia se reduce a 7 cm.
- En el caso de pisoductos o caños metálicos, la circulación puede ser en conductos contiguos.
- Si es inevitable cruzar un gabinete de distribución con energía , no debe circularse paralelamente a más de un lateral.
- De usarse cañerías plásticas, lubricar los cables (talco industrial, vaselina, etc) para reducir la fricción entre los cables y las paredes de los caños ya que esta genera un incremento de la temperatura que aumenta la adherencia.
- El radio de las curvas no debe ser inferior a 2”.
- Las canalizaciones no deben superar los 20 metros o tener más de 2 cambios de dirección sin 18 cajas de paso .
- En tendidos verticales se deben fijar los cables a intervalos regulares para evitar el efecto del peso en el acceso superior.
- Al utilizar fijaciones (grampas, precintos o zunchos) no excederse en la presión aplicada (no arrugar la cubierta), pues puede afectar a los conductores internos.

A.4.1.8 Recomendaciones en Cuanto a la Documentación

La administración del sistema de cableado incluye la documentación de los cables, terminaciones de los mismos, cruzadas, paneles de “patcheo”, armarios de telecomunicaciones y otros espacios ocupados por los sistemas de telecomunicaciones. La documentación es un componente de la máxima importancia para la operación y el mantenimiento de los sistemas de telecomunicaciones. Resulta importante poder disponer, en todo momento, de la documentación actualizada, y fácilmente actualizable, dada la gran variabilidad de las instalaciones debido a mudanzas, incorporación de nuevos servicios, expansión de los existentes,etc. En particular, es muy importante proveerlos de planos de todos los pisos, en los que se datallen:

- Ubicación de los gabinetes de telecomunicaciones
- Ubicación de ductos a utilizar para cableado vertical
- Disposición de tallada de los puestos eléctricos en caso de ser requeridos

- Ubicación de pisoductos si existen y pueden ser utilizados.

A.4.1.9 Normas y Estándares

Una entidad que compila y armoniza diversos estándares de telecomunicaciones es la Building Industry Consulting Service International (BiCSi). El Telecommunications Distribution Methods Manual (TDMM) de BiCSi establece guías pormenorizadas que deben ser tomadas en cuenta para el diseño adecuado de un sistema de cableado estructurado. El Cabling Installation Manual establece las guías técnicas, de acuerdo a estándares, para la instalación física de un sistema de cableado estructurado.

El Instituto Americano Nacional de Estándares, la Asociación de Industrias de Telecomunicaciones y la Asociación de Industrias Electrónicas (ANSI/TIA/EIA) publican conjuntamente estándares para la manufactura, instalación y rendimiento de equipo y sistemas de telecomunicaciones y electrónico. Cinco de éstos estándares de ANSI/TIA/EIA definen cableado de telecomunicaciones en edificios. Cada estándar cubre un parte específica del cableado del edificio. Los estándares establecen el cable, hardware, equipo, diseño y prácticas de instalación requeridas. Cada estándar ANSI/TIA/EIA menciona estándares relacionados y otros materiales de referencia.

La mayoría de los estándares incluyen secciones que definen términos importantes, acrónimos y símbolos. Los cinco estándares principales de ANSI/TIA/EIA que gobiernan el cableado de telecomunicaciones en edificios son:

- ANSI/TIA/EIA-568-A, Estándar de Cableado de Telecomunicaciones en Edificios Comerciales.
- ANSI/TIA/EIA-569, Estándar para Ductos y Espacios de Telecomunicaciones en Edificios Comerciales.
- ANSI/TIA/EIA-570, Estándar de Alambrado de Telecomunicaciones Residencial y Comercial Liviano.
- ANSI/TIA/EIA-606, Estándar de Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales.

- ANSI/TIA/EIA-607, Requerimientos para Telecomunicaciones de Puesta a Tierra y Puenteado de Edificios Comerciales.
- El National Electrical Code 1996(NEC), ANSI/NFPA-70 publicado por la National Fire Protection Agency (NFPA), proporciona los estándares de seguridad eléctrica que protegen a personas y a la propiedad de fuego y riesgos eléctricos. La última edición del NEC es la de 1996. Cada tres años se publican versiones nuevas del NEC. En Costa Rica el código eléctrico publicado por el Colegio Federado de Ingenieros y Arquitectos es el Código Eléctrico de Costa Rica (CODEC). La última versión del CODEC data de 1992.

Existen estándares adicionales que también deben ser tomados en cuenta a la hora de definir o diseñar un sistema de telecomunicaciones.

Documentos adicionales:

- Manual de Métodos de Distribución de Telecomunicaciones del Building Industry Consulting Service Internacional.
- ANSI/TIA/EIA TSB-36, Especificaciones Adicionales para Cables de Par Trenzado sin Blindaje. Esta especificación se define por aparte de ANSI/TIA/EIA-568 pero se incluye en el ANSI/TIA/EIA-568-A.
- ANSI/TIA/EIA TSB-40, Especificaciones Adicionales de Transmisión para Hardware de Conexión de Cables de Par Trenzado sin Blindaje. Esta especificación se define por aparte de ANSI/TIA/EIA-568 pero se incluye en ANSI/TIA/EIA-568-A.
- ANSI/TIA/EIA TSB-67, Especificación para la Prueba en el Campo del Rendimiento de Transmisión de Sistemas de Cableado de Par Trenzado sin Blindaje.
- ANSI/TIA/EIA TSB-72, Guía para el Cableado de Fibra Optica Centralizada.
- ANSI/EIA 310-D-92, Gabinetes, Andenes, Páneles y Equipo Asociado.
- NFPA-75 (Edición 1995), Estándar para la Protección de Equipo de Cómputo Electrónico y de Procesamiento de Datos.
- NFPA-780 (Edición 1995), Estándar para la Instalación de Sistemas de Protección Contra Rayos.
- Documentos y panfletos de Panduit Network Systems.

A.5 HARDWARE

A.5.1 Switch Cisco Catalyst 2950

Caracteristicas:

- Switch de acceso Fast Ethernet.
- Permite la migración a Gigabit sobre diversidad de medios.
- Almacena hasta 8.000 direcciones MAC.

Permite implementar:

- QoS
- Administración de tráfico Multicast.
- Posibilita servicios avanzados Cisco IOS.
- Soporta Cisco Redundant Power System 300.

Soporta managment:

- In-band con SNMP o telnet.
- Out-band a través del puerto consola.

	Configuración Hardware	Puertos	
Catalyst 2950-12	Fija	12 10/100 autosensing	2950G-12 - 2 puertos 1000 Base X*
Catalyst 2950-24	Fija	24 10/100 autosensing	2950C-24 - 2 puertos 100 BaseFX 2950T-24 - 2 puertos 1000 Base T 2950G-24 - 2 puertos 1000 Base X*

GLOSARIO

ACK

Acuse de recibo. Notificación que se envía desde un dispositivo de red a otro para acusar recibo de que se ha producido algún evento (por ejemplo, que se ha recibido un mensaje). A veces se abrevia como ACK.

Anillo

Conexión de una o más estaciones en una topología lógicamente circular. La información se envía de forma secuencial entre las estaciones activas. Token Ring, FDDI y CDDI se basan en esta topología.

Atenuación

Pérdida de la energía de la señal de comunicación.

ATM

Modo de transferencia asíncrona. El estándar internacional para relay de celdas en las que múltiples tipos de servicio (como, por ejemplo, voz, vídeo o datos) se transmiten en celdas de longitud fija (53 bytes). Las celdas de longitud fija permiten que el procesamiento de celdas se lleve a cabo en el hardware, disminuyendo por lo tanto los retardos en el tránsito. ATM está diseñada para sacar provecho de los medios de transmisión de alta velocidad como, por ejemplo, E3, SONET y T3.

Banda ancha

Sistema de transmisión que permite multiplexar múltiples señales independientes en un cable. En la terminología de telecomunicaciones, cualquier canal que tenga un ancho de banda mayor que el de un canal con calidad de voz (4 kHz). En terminología LAN, un cable coaxial en el que se usa la señalización analógica.

Banda base

Característica de una tecnología de red en la que se usa sólo una frecuencia de portadora. Ethernet es un ejemplo de una red de banda base. También denominada banda estrecha.

Baudio

Unidad de velocidad de señalización que es igual a la cantidad de elementos discretos de la señal transmitidos por segundo. Baudio es sinónimo de bits por segundo (bps), si cada elemento de la señal representa exactamente 1 bit.

Bit

Dígito binario que se usa en el sistema de numeración binario. Puede ser 0 ó 1.

Broadcast

Paquete de datos que se envía a todos los nodos de una red. Los broadcasts se identifican a través de una dirección de broadcast.

Cable

Medio de transmisión de hilo de cobre o fibra óptica envuelto en una cubierta protectora.

Cableado backbone

Cableado que proporciona interconexiones entre los armarios de cableado, entre los centros de cableado y el POP, y entre los edificios que forman parte de la misma LAN.

Canal lógico

Ruta de comunicación conmutada por paquetes, no dedicada, entre dos o más nodos de red. La conmutación por paquetes permite que existan varios canales lógicos de forma simultánea en un solo canal físico.

Checksum (suma de verificación)

1) Método para controlar la integridad de los datos transmitidos. La checksum es el valor de un número entero que se calcula a partir de una secuencia de octetos a través de una serie de operaciones aritméticas. El valor se vuelve a calcular en el extremo receptor y se compara para verificarlo.
2) La checksum calculada del encabezado y de los campos de datos.

Circuito

Ruta de comunicación entre dos o más puntos.

Circuito virtual

Circuito lógico que se crea para garantizar la comunicación confiable entre dos dispositivos de red. Un circuito virtual se define por un par VPI/VCI, y puede ser permanente (un PVC) o conmutado (un SVC).

Cisco Discovery Protocol

Protocolo de descubrimiento de dispositivos independiente de los medios y protocolos que se ejecuta en todos los equipos fabricados por Cisco, incluyendo routers, servidores de acceso, puentes y switches. Al usar CDP, el dispositivo puede advertir de su existencia a otros dispositivos y recibir información acerca de otros dispositivos en la misma LAN o en el lado remoto de una WAN. Se ejecuta en todos los medios que admitan SNAP, incluyendo las LAN, Frame Relay y ATM.

CiscoWorks

Conjunto de aplicaciones de software para administración de internetwork basadas en SNMP. CiscoWorks incluye aplicaciones para monitorear el estado del router y del servidor de acceso, gestionar los archivos de configuración y diagnosticar los problemas de las redes. Las aplicaciones CiscoWorks se integran en varias plataformas de administración de red basadas en SNMP, incluyendo SunNet Manager, HP OpenView e IBM NetView.

Colisión

En Ethernet, el resultado de dos nodos que transmiten de forma simultánea. Las tramas de cada uno de los dispositivos chocan y resultan dañadas cuando se encuentran en el medio físico.

Dirección de red

Dirección de capa de red que se refiere a un dispositivo de red lógico, más que físico. También denominada dirección de protocolo.

ELAN

LAN emulada. Red ATM en la que se emula una LAN Ethernet o Token Ring utilizando un modelo cliente-servidor. Las ELAN están compuestas por un LEC, un LES, un BUS y un LECS.

Pueden existir múltiples ELAN en una sola red ATM de forma simultánea. Las ELAN se definen a través de la especificación LANE. Ver también BUS, LANE, LEC, LECS y LES.

Fibra local 4B/5B

Fibra local de 4 bytes/5 bytes. Medio físico del canal de fibra que se usa para FDDI y ATM. Admite velocidades de hasta 100 Mbps a través de fibra multimodo. Ver también TAXI 4B/5B.

Fibra local 8B/10B

Fibra local de 8 bytes/10 bytes. Medio físico del canal de fibra que admite velocidades de hasta 149.76 Mbps a través de fibra multimodo.

Fibra monomodo

Cable de fibra óptica con un núcleo estrecho que permite que la luz entre sólo en un único ángulo. Dicho cableado tiene mayor ancho de banda que la fibra multimodo, pero requiere una fuente de luz con una anchura espectral más angosta (por ejemplo, un láser). También denominada fibra de modo único.

Fibra multimodo

Fibra óptica que permite la propagación de múltiples frecuencias de luz.

Full duplex

Capacidad de transmitir datos de forma simultánea entre una estación emisora y una estación receptora.

Grupo de trabajo

Conjunto de estaciones de trabajo y servidores de una LAN que están diseñados para comunicarse e intercambiar datos entre sí.

Half duplex

Capacidad de transmitir los datos en una sola dirección a la vez entre una estación emisora y una estación receptora.

Host

Sistema computacional ubicado en una red. Es similar al término nodo, salvo que el host generalmente implica un sistema computacional, mientras que el nodo generalmente se aplica a cualquier sistema conectado a la red, incluyendo servidores de acceso y routers.

Internetwork

Conjunto de redes interconectadas por routers y otros dispositivos que funcionan (generalmente) como una sola red. A veces denominada internet, que no se debe confundir con la Internet.

Internetworking

Término general que se usa para referirse a la industria que ha surgido alrededor del problema de conectar redes entre sí. El término puede referirse a productos, procedimientos y tecnologías.

Latencia

1) Retardo entre el momento en que el dispositivo solicita acceso a una red y el momento en el que se le otorga permiso para transmitir.
2) Retardo entre el momento en que un dispositivo recibe una trama y el momento en que la trama sale desde el puerto destino.

Loop

Ruta en la que los paquetes nunca llegan a destino, sino que simplemente hacen bucles repetitivos a través de un conjunto constante de nodos de red.

MBONE

Backbone multicast. El backbone multicast de Internet. MBONE es una red virtual multicast compuesta por LAN multicast y túneles punto a punto que las interconectan.

Multicast

Paquetes individuales que la red copia y envía a un subconjunto específico de direcciones de red. Estas direcciones se especifican en el campo de dirección destino. Comparar con broadcast y unicast.

NAP

Punto de acceso a la red. Ubicación donde se produce la interconexión de proveedores de servicio de Internet en los Estados Unidos de Norteamérica para el intercambio de paquetes.

Networking

Conexión de cualquier conjunto de computadores, impresoras, routers, switches y otros dispositivos con el propósito de comunicarse a través de algún medio de transmisión.

Portadora

Onda electromagnética o corriente alterna de una sola frecuencia, adecuada para modulación por parte de otra señal portadora de datos.

Simplex

Capacidad de transmitir los datos en una sola dirección entre una estación emisora y una estación receptora.

Socket

Estructura de software que opera como un punto de terminación de comunicaciones dentro de un dispositivo de red.

Software Cisco IOS

(Software del sistema operativo de internetworking de Cisco). Software del sistema Cisco que brinda funcionalidad, escalabilidad y seguridad común para todos los productos de la arquitectura CiscoFusion. El software Cisco IOS permite instalación y administración centralizada, integrada y automatizada de internetworks, garantizando al mismo tiempo soporte para una amplia variedad de protocolos, medios, servicios y plataformas. Ver también CiscoFusion.

Topología

Disposición física de los nodos y medios de red dentro de una estructura de networking empresarial.

Trama

Agrupación lógica de información que se envía como una unidad de capa de enlace de datos a través de un medio de transmisión. A menudo, se refiere al encabezado y a la información final, que se usan para la sincronización y el control de errores, que rodean a los datos del usuario contenidos en la unidad. Los términos datagrama, mensaje, paquete y segmento también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

Unicast

Mensaje que se envía a un solo destino de red.

VLAN

LAN virtual. Grupo de dispositivos en una LAN que se configuran (usando software de administración) de modo que se puedan comunicar como si estuvieran conectadas al mismo cable cuando, de hecho, están ubicadas en una cantidad de segmentos LAN distintos. Dado que las VLAN se basan en conexiones lógicas y no físicas, son extremadamente flexibles.