# UNIVERSIDAD NACIONAL DEL CALLAO
# FACULTAD DE INGENIERIA ELECTRICA Y ELECTRONICA


## DISEÑO E IMPLEMENTACION DE L SISTEMA DE INFORMACIÓN VIA INTRANET EN EL HOSPITAL DE APOYO "JAMO" - TUMBES

**PRESENTADA POR:**
**Bach. PEDRO ALEJANDRO TORIBIO PASAPERA**

**Callao – 2005**

**“DISEÑO E IMPLEMENTACION DEL SISTEMA DE INFORMACIÓN VIA INTRANET EN EL HOSPITAL DE APOYO JAMO-TUMBES”**

**Tesis para obtener el Título Profesional de Ingeniero Electrónico**

**ASESORADO POR:**
**ING. VICTOR GUTIERREZ TOCAS.**

**CALLAO - PERU**

***A mis padres Carmen y Rubén,***
***y mi ángel de la guarda, mi Abuela Bernavita.***

## AGRADECIMIENTO

Agradezco el apoyo considerado por parte del Ing. Víctor Gutiérrez Tocas, Asesor de mi Tesis, por su apoyo desinteresado para con mi proyecto.

Que con sus opiniones y sugerencias he podido desarrollar y aplicar el presente trabajo, como base para la Implementación de un Sistema de Información Vía Intranet en el Hospital de Apoyo “JAMO” – Tumbes.

# INDICE

# LISTA DE FIGURAS

# CAPITULO I

## 1.1 INTRODUCCION

En la actualidad, en casi todos los países de la Región existen deficiencias graves en la organización de la atención e investigación de salud, que se expresan como instituciones de alta complejidad sobrecargados de casos sencillos que podrían tratarse con un costo menor en establecimientos más accesibles, falta de accesibilidad a servicios especializados y tecnológicos.

En nuestro país, como en muchas naciones que han alcanzado una situación intermedia de desarrollo en servicios e investigación de salud, es necesario definir un modelo global de organización de atención e investigación de salud según niveles de complejidad progresiva, cuyos recursos humanos, físicos y tecnológicos deberían ser determinados; y normalizados de manera que garanticen la existencia, en esos niveles, de una atención con capacidad resolutiva conocida.

Por ello este estudio, responde a las necesidades de muchas instituciones de servicios e investigación de salud de nuestro país, desde establecer los criterios normativos del Diseño e Implementación del Sistema de Información Vía Intranet, el cual se basa en estándares internacionales que deberían observarse con mucha importancia.

El presente estudio, brinda una solución de una Red de Comunicaciones, para interconectar los servicios internos y externos de una red privada, con características de instalaciones normativas, reconfigurable, estandarizado y universales, capaz de soportar los servicios y aplicaciones de

Voz, Data y Video, con un grado de seguridad en el servicio de comunicación de la red.

## 1.2 OBJETIVOS

### OBJETIVOS GENERALES

- Diseñar e Implementar el servicio de datos, así brindar las posibilidades de una alternativa de los servicios de voz y video.
- Entregar estudio de campo y los costos detallados del proyecto, para su ejecución e implementación.

### OBJETIVOS ESPECIFICOS

- Realizar un catastro de los equipos de conmutación existentes dentro del Hospital de Apoyo “JAMO - Tumbes”, para si tener la base en que se desarrollará el proyecto.
- El Sistema de Comunicación de Datos es fundamental en toda institución, pero debemos tener en cuenta el avance e importancia de los Sistemas de Telefonía y Videoconferencia.
- Asignar un Centro de Telecomunicaciones de la cual se derivara el sistema de cableado estructurado.
- Conocer los conceptos básicos y técnicos para el Sistema de Información Vía Intranet.
- Dar la presentación fundamental de la importancia de una Red de Información.
- Diferenciar las ventajas y desventajas de las tecnologías existentes para una red de información.

## 1.3 ANTECEDENTES Y JUSTIFICACIÓN

El Hospital de Apoyo “JAMO”, desde su creación hasta la actualidad ha buscado la manera de brindar un servicio de calidad y más aún en los últimos años con el desarrollo apresurado de los nuevos avances tecnológicos en el que se hace uso de los medios de comunicación principalmente, es entonces que nace la necesidad de la transferencia de datos por medio de una red de comunicaciones conmutada, el hospital cuenta con instalaciones Administrativas, de Operaciones, y Servicios Médicos - Hospitalarios, de un solo nivel de construcción expandida, en la ciudad de Tumbes.

Presenta una red de comunicaciones de baja calidad y seguridad de servicio, sin central telefónica, sistema de instalaciones eléctricas muy antiguas e inestables.

Por estas razones se pretende Diseñar e Implementar un Sistema de Comunicaciones, para así contar con un servicio más eficiente y de calidad, entre los distintos servicios del hospital.

# CAPITULO II

## 2.1 ESTUDIO DEL ARTE Y DISEÑO

El Hospital de Apoyo “JAMO” en la ciudad de Tumbes, forma parte del Ministerio de Salud, el cual esta conformado por una amplia gama de hospitales en todo el país. El Hospital cuenta con más de 2500 camas atendidas por médicos, enfermeros y resto de personal sanitario que superan las 150 personas.

La red de comunicaciones interna, como servicio básico debe dotar al hospital de los medios de comunicación necesarios para que el personal pueda desarrollar sus funciones como hospital moderno.

Los beneficios de integrar todos los servicios en una sola red suponen un mejor aprovechamiento de la infraestructura, una reducción del equipamiento a instalar y mantener, y el disponer de un Centro de Gestión de Red unificado. Todo ello redunda en un ahorro de costos y en una amortización más rápida de infraestructura instalada.

En una red multiservicio, nos encontramos con diferentes terminales de acceso totalmente diferentes entre sí, desde teléfonos convencionales, centralitas, ordenadores de usuarios, impresoras, servidores, equipos de videoconferencia, etc.

Cada uno de estos equipos accede a la red a través de un medio diferente, pares de cobre para teléfonos, cableado estructurado para las computadoras y enlaces de cobre o fibra para los equipos de telemedicina y de videoconferencia; evidentemente con protocolos diferentes predominando

TCP/IP sobre redes locales Ethernet para los entornos de computadoras y ATM para los entornos de equipos de telemedicina.

Además de la comunicación interna del hospital, es necesaria la comunicación con el resto de hospitales del Ministerio de Salud, con otros Centros Sanitarios y en general con el resto del mundo a través de Internet.

Para el Diseño de la red, se tuvo los principales criterios:

- Gran variedad de equipamiento de acceso a red.
- Construcción de un “Backbone” que soporte todo el tráfico generado por dichos equipos.
- Garantizar diferentes calidades de servicio que posibiliten que los diferentes servicios coexistan entre sí.
- Dotar a todo el conjunto de las medidas de seguridad y redundancia necesarias para entornos críticos que garanticen disponibilidad de la red 7 días a la semana y 24 horas al día.
- Accesos con el exterior del hospital, con otros hospitales del mundo y con la red corporativa del Ministerio de Salud.

Estos criterios, nos permitirá brindar los siguientes servicios:

- Atención personalizada al paciente.
- Facilidad de acceso a la información.
- Accesos a bases de datos internos y otros hospitales.
- Transmisión en tiempo real de intervenciones, consultas y exploraciones desde diferentes puntos del hospital.
- Transmisión de conferencias, charlas o reuniones desde distintas ubicaciones dentro o fuera del hospital.

- Formación y Capacitación a distancia.

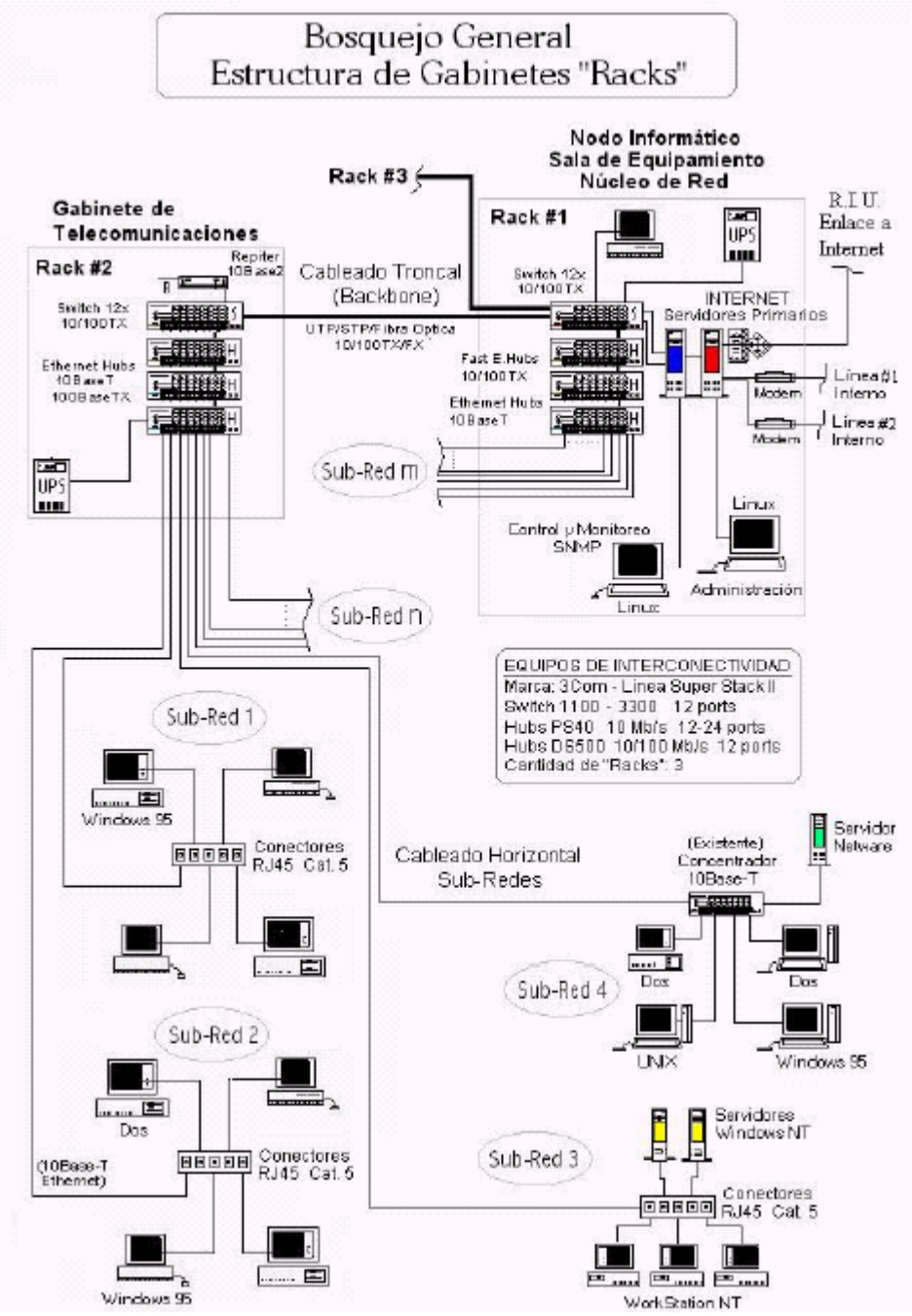



***Figura Nº 01 Diagrama de una Red Privada (Intranet)***

## 2.2 REDES Y TECNOLOGIAS

El término red de computadoras se refiere a una colección interconectada de computadoras autónomas. Se dice que dos computadoras están interconectadas si son capaces de intercambiar información. Por otra parte, si una computadora puede controlar otra a voluntad, las computadoras no son autónomas.

### 2.2.1. Tecnologías Existentes

#### 2.2.1.1. Redes para Instituciones

En términos generales, la cuestión aquí es compartir los recursos y la meta es hacer que todos los programas, el equipo y especialmente los datos estén disponibles para cualquiera en la red, sin importar la localización física de los recursos y de los usuarios.

Una segunda meta es lograr una alta confiabilidad al contar con fuentes alternativas de suministro. La capacidad para seguir operando pese a problemas de *hardware* es de suma importancia.

Otro objetivo es la de ahorrar dinero. Es por eso que muchos diseñadores construyan sistemas compuestos por computadoras personales, una por usuario, con los datos guardados en una o más máquinas servidoras de archivos compartidas. En este modelo, los usuarios se denominan clientes, y el arreglo completo se llama modelo cliente-servidor. En este modelo, la comunicación generalmente adopta la forma de un mensaje de solicitud del cliente al servidor pidiendo que se efectúe algún trabajo. A continuación, el servidor hace el trabajo y devuelve la respuesta.

Otra meta al establecer redes es la escalabilidad: la capacidad para incrementar el rendimiento del sistema gradualmente cuando la carga de trabajo crece. Con el modelo cliente-servidor se pueden añadir nuevos clientes y nuevos servidores cuando es necesario.

Una red de computadoras puede proporcionar un potente medio de comunicación. Esta cualidad proporciona facilidad de cooperación entre grupos de gente alejados físicamente.

#### 2.2.1.2. Redes para Usuarios

Uno de los aspectos a considerar en este tipo de redes es el acceso a la información remota, la cual vendrá dada en muchas formas. Ésta es la primera categoría existente dentro de este tipo de redes. Una aplicación ubicada dentro de esta categoría es la actual red mundial de información (*World Wide Web*). Todas las aplicaciones dentro de esta categoría implican la interacción entre una persona y una base de datos remota aunque también las hay que implican interacción entre persona y persona. Ésta será, entonces, la segunda categoría existente.

Algunas de estas aplicaciones son muy conocidas como puede ser el correo electrónico mediante el cual dos personas (o más) pueden enviarse mensajes como modo de intercambiar información. Un derivado de este, cuando se lleva a cabo en tiempo real, es la videoconferencia que posibilita la realización de reuniones virtuales entre personas geográficamente alejadas.

La tercera y última categoría es la relacionada con el entretenimiento. Dentro de aproximadamente una década, será posible seleccionar cualquier película o programa de televisión creado en cualquier país y exhibirlo en la

pantalla de forma instantánea. Algunas películas llegarán a ser interactivos, preguntándose al usuario (en momentos puntuales) qué dirección debe seguir la historia con argumentos alternativos para todos los casos. La televisión en directo también puede llegar a ser interactivo, con la audiencia participando en concursos, escogiendo entre los concursantes existentes, etc. Dentro de este mismo campo aparecerán los videojuegos a la carta donde los jugadores podrán jugar contra otros geográficamente alejados.

En pocas palabras, la capacidad para combinar información, comunicación y entretenimiento seguramente hará surgir una nueva y enorme industria basada en las redes de computadoras.

### 2.2.2. Tecnología de Transmisión

No existe una clasificación aceptada dentro de la cual quepan todas las redes de computadoras, pero dos diferencias sobresalen como más importantes: la tecnología de transmisión y la escala.

En términos generales, hay dos tipos de tecnología de transmisión: las redes de difusión y las redes punto a punto.

Las redes de difusión tienen un solo canal de comunicación compartido por todas las máquinas de la red. Los mensajes que envía una máquina son recibidos por todas las demás.

Un campo de dirección dentro de este mensaje especifica a quién se dirige. Al recibir el mensaje, una máquina verifica el campo de dirección para determinar si va dirigido a ella. Si es así, lo procesa; si va dirigido a cualquier otra máquina, lo ignora.

Los sistemas de difusión (generalmente) también ofrecen la posibilidad de dirigir un mensaje a todos los destinos para lo cual se coloca como dirección de destino un código especial que no corresponde con ninguna de las direcciones de las restantes máquinas. Cuando se transmite un mensaje con este código, cada máquina de la red lo recibe y lo procesa. Este modo de operación se llama difusión (*broadcasting*). Algunos sistemas de difusión también contemplan la transmisión a un subconjunto de las máquinas de la red, algo conocido con el nombre de multidifusión.

En contraste, las redes punto a punto consisten en muchas conexiones entre pares individuales de máquinas. Para ir del origen al destino; un mensaje, en este tipo de red, puede tener que visitar primero una o varias máquinas intermedias. A veces son posibles múltiples rutas de diferentes longitudes (consecuentemente, retardos), por lo que los algoritmos de ruteo desempeñan un papel importante en las redes punto a punto.

Como regla general (aunque hay muchas excepciones), las redes pequeñas geográficamente localizadas tienden a usar difusión, mientras que las redes más grandes suelen ser punto a punto.

Un criterio alternativo para clasificar las redes es su escala. En las verdaderas redes, las computadoras se comunican intercambiando mensajes por cables largos. Estas pueden dividirse en redes locales, metropolitanas y de área amplia. Finalmente, hay que comentar que la interconexión de dos o más redes (iguales o distintas) forma una inter-red.

### 2.2.3. Tipos de Redes

#### 2.2.3.1. Redes de Área Local - LAN

Las redes de Área Local, generalmente llamadas LAN (*Local Área Network*), son redes de propiedad privada dentro de un solo edificio o campus de hasta unos cuantos kilómetros de extensión. Se usan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de compañías y fábricas con objeto de compartir recursos (por ejemplo, impresoras) e intercambiar información.

Las LAN están restringidas en tamaño, lo cual significa que el tiempo de transmisión del peor caso está limitado y se conoce de antemano. Conocer este límite hace posible usar ciertos tipos de diseños que de otra manera no serían prácticos, y también simplifica la administración de la red.

#### 2.2.3.2. Redes LAN Ethernet

Ethernet es la tecnología de red LAN más usada, resultando idóneas para aquellos casos en los que se necesita una red local que deba transportar tráfico esporádico y ocasionalmente pesado a velocidades muy elevadas. Las redes Ethernet se implementan con una topología física de estrella y lógica de bus, y se caracterizan por su alto rendimiento a velocidades de 10-100 Mbps

El origen de las redes Ethernet hay que buscarlo en la Universidad de Hawai, donde se desarrollo, en los años setenta, el **Método de Acceso Múltiple con Detección de Portadora y Detección de Colisiones, CSMA/CD** (Carrier Sense and Multiple Access with Collition Detection), utilizado actualmente por Ethernet. Este método surgió ante la necesidad de

implementar en las islas Hawai un sistema de comunicaciones basado en la transmisión de datos por radio, que se llamó Aloha, y permite que todos los dispositivos puedan acceder al mismo medio, aunque sólo puede existir un único emisor encada instante. Con ello todos los sistemas pueden actuar como receptores de forma simultánea, pero la información debe ser transmitida por turnos.

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

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

Una colisión se produce pues cuando dos máquinas escuchan para saber si hay tráfico de red, no lo detectan y, acto seguido transmiten de forma simultánea. En este caso, ambas transmisiones se dañan y las estaciones deben volver a transmitir más tarde.

Para intentar solventar esta pérdida de paquetes, las máquinas poseen mecanismos de detección de las colisiones y algoritmos de postergación que

determinan el momento en que aquellas que han enviado tramas que han sido destruidas por colisiones pueden volver a transmitirlas.

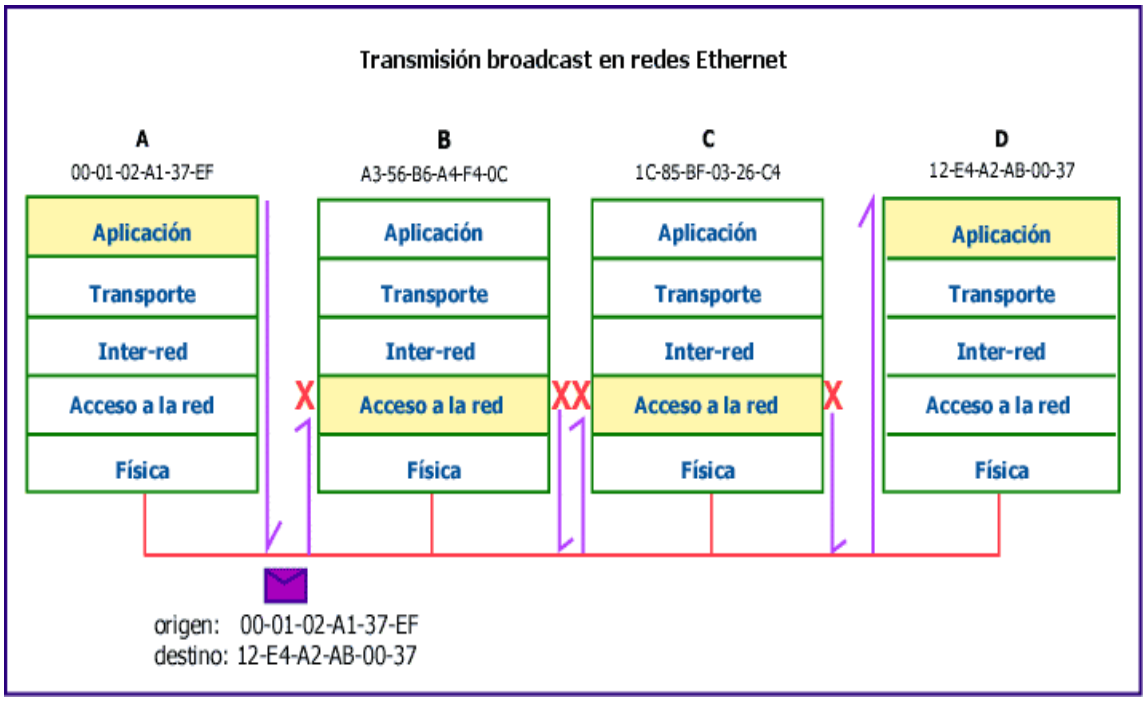



Figura Nº 02 Modo Transmisión Broadcast - Ethernet

Existen dos especificaciones diferentes para un mismo tipo de red, Ethernet y IEEE 802.3. Ambas son redes de broadcast, lo que significa que cada máquina puede ver todas las tramas, aunque no sea el destino final de las mismas. Cada máquina examina cada trama que circula por la red para determinar si está destinada a ella. De ser así, la trama pasa a las capas superiores para su adecuado procesamiento. En caso contrario, la trama es ignorada.

Ethernet proporciona servicios correspondientes a la capas física y de enlace de datos del modelo de referencia OSI, mientras que IEEE 802.3 especifica la capa física y la porción de acceso al canal de la capa de enlace de datos, pero no define ningún protocolo de Control de Enlace Lógico.

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

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

Tanto Ethernet como IEEE 802.3 se implementan a través de la tarjeta de red o por medio de circuitos en una placa dentro del host.

**Formato de trama Ethernet**

Según hemos visto, los datos generados en la capa de aplicación pasan a la capa de transporte, que los divide en segmentos, porciones de datos aptas para su transporte por res, y luego van descendiendo pos las sucesivas capas hasta llegar a los medios físicos. Conforme los datos van bajando por la pila de capas, paso a paso cada protocolo les va añadiendo una serie de cabeceras y datos adicionales; necesarios para poder ser enviados a su destino correctamente. El resultado final es una serie de unidades de información denominadas tramas, que son las que viajan de un host a otro.

La forma final de la trama obtenida, en redes Ethernet, es la siguiente:

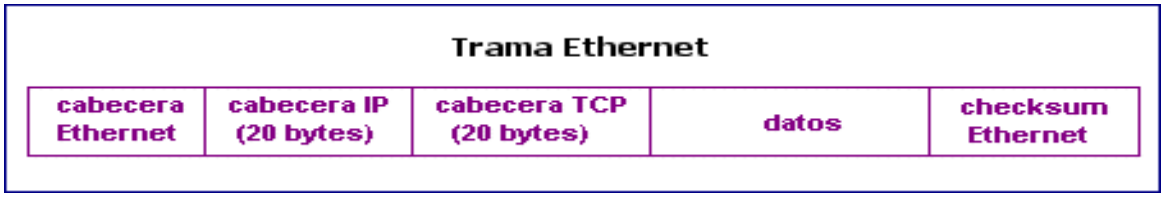



Figura Nº 03 Trama Ethernet

Y los principales campos que la forman son:

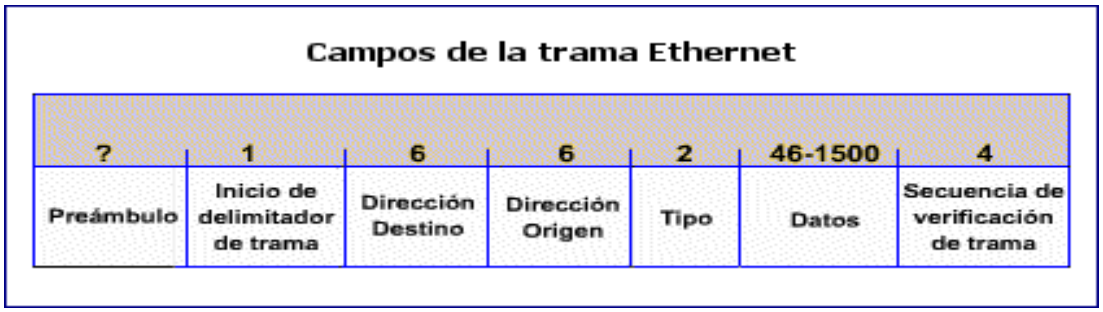



Figura Nº 04 Campos de la Trama Ethernet

- Preámbulo: Patrón de unos y ceros que indica a las estaciones receptoras que una trama es Ethernet o IEEE 802.3. La trama Ethernet incluye un byte adicional que es el equivalente al campo Inicio de Trama (SOF) de la trama IEEE 802.3.
- Inicio de trama (SOF): Byte delimitador de IEEE 802.3 que finaliza con dos bits 1 consecutivos, y que sirve para sincronizar las porciones de recepción de trama de todas las estaciones de la red. Este campo se especifica explícitamente en Ethernet.
- Direcciones destino y origen: Incluye las direcciones físicas (MAC) únicas de la máquina que envía la trama y de la máquina destino. La dirección origen siempre es una dirección única, mientras que la de destino puede ser de broadcast única (trama enviada a una sola máquina), de broadcast múltiple (trama enviada a un grupo) o de broadcast (trama enviada a todos los nodos).
- Tipo (Ethernet): Especifica el protocolo de capa superior que recibe los datos una vez que se ha completado el procesamiento Ethernet.

- Longitud (IEEE 802.3): Indica la cantidad de bytes de datos que sigue este campo.
- Datos: Incluye los datos enviados en la trama. En las especificación IEEE 802.3, si los datos no son suficientes para completar una trama mínima de 64 bytes, se insertan bytes de relleno hasta completar ese tamaño (tamaño mínimo de trama). Por su parte, las especificaciones Ethernet versión 2 no especifican ningún relleno, Ethernet espera por lo menos 46 bytes de datos.
- Secuencia de verificación de trama (FCS): Contiene un valor de verificación CRC (Control de Redundancia Cíclica) de 4 bytes, creado por el dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas.

Cuando un paquete es recibido por el destinatario adecuado, les retira la cabecera de Ethernet y el checksum de verificación de la trama, comprueba que los datos corresponden a un mensaje IP y entonces lo pasa a dicho protocolo para que lo procese. El tamaño máximo de los paquetes en las redes Ethernet es de 1500 bytes.

**Tipos de Redes Ethernet**

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

**Variedades de red Ethernet**

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

Figura Nº 05 Tipos de Red Ethernet

Las tecnologías Ethernet más comunes y más importantes son:

- **Ethernet 10Base2.** Usa un cable coaxial delgado, por lo que se puede doblar más fácilmente, y además es más barato y fácil de instalar, aunque los segmentos de cable no pueden exceder de 200 metros y 30 nodos. Las conexiones se hacen mediante *conectores en T*, más fáciles de instalar y más seguros.
- **Ethernet 10Base5.** También llamada Ethernet gruesa, usa un cable coaxial grueso, consiguiendo una velocidad de 10 Mbps Puede tener hasta 100 nodos conectados, con una longitud de cable de hasta 500 metros. Las conexiones se hacen mediante la técnica denominada

*derivaciones de vampiro*, en las cuales se inserta un polo hasta la mitad del cable, realizándose la derivación en el interior de un transceiver, que contiene los elementos necesarios para la detección de portadores y choques. El transceiver se une al computador mediante un cable de hasta 50 metros.

- **Ethernet 10Base-T.** Cada estación tiene una conexión con un hub central, y los cables usados son normalmente de par trenzado. Son las LAN más comunes hoy en día. Mediante este sistema se palian los conocidos defectos de las redes 10BAse2 y 10Base5, a saber, la mala detección de derivaciones no deseadas, de rupturas y de conectores flojos. Como desventaja, los cables tienen un límite de sólo 100 metros, y los hubs pueden resultar caros.
- **Ethernet 10Base-FX.** Basada en el uso de fibra óptica para conectar las máquinas, lo que la hace cara para un planteamiento general de toda la red, pero idónea para la conexión entre edificios, ya que los segmentos pueden tener una longitud de hasta 2000 metros, al ser la fibra óptica insensible a los ruidos e interferencias típicos de los cables de cobre. Además, su velocidad de transmisión es mucho mayor.
- **Fast Ethernet**. Las redes 100BaseFx (IEEE 802.3u) se crearon con la idea de paliar algunos de los fallos contemplados en las redes Ethernet 10Base-T y buscar una alternativa a las redes FDDI Son también conocidas como redes Fast Ethernet, y están basadas en una topología en estrella para fibra óptica. Con objeto de hacerla compatible con Ethernet 10Base-T, la tecnología Fast Ethernet preserva los formatos de los paquetes y las interfaces, pero aumenta la rapidez de transmisión

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

#### 2.2.3.3. Redes LAN Token Ring

Las redes Token Ring son redes de tipo determinista, al contrario de las redes Ethernet. En ellas, el acceso al medio está controlado, por lo que solamente puede transmitir datos una máquina por vez, implementándose este control por medio de un token de datos, que define qué máquina puede transmitir en cada instante. Token Ring e IEEE 802.5 son los principales ejemplos de redes de transmisión de tokens.

Las redes de transmisión de tokens se implementan con una topología física de estrella y lógica de anillo, y se basan en el transporte de una pequeña trama, denominada token, cuya posesión otorga el derecho a transmitir datos. Si un nodo que recibe un token no tiene información para enviar, transfiere el token al siguiente nodo. Cada estación puede mantener al token durante un período de tiempo máximo determinado, según la tecnología específica que se haya implementado.

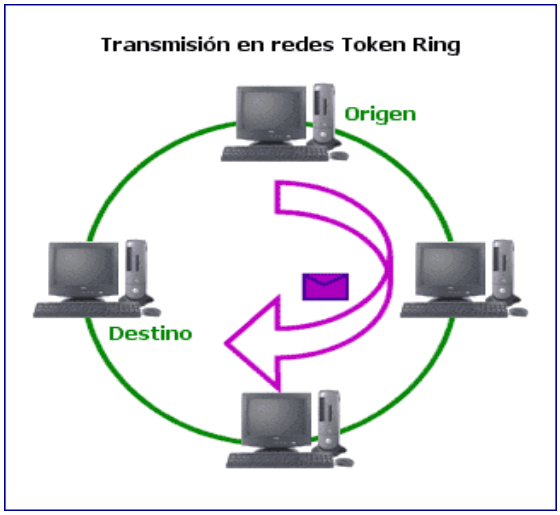



Figura Nº 06 Transmisión – Redes Token Ring

Cuando una máquina recibe un token y tiene información para transmitir, toma el token y le modifica un bit, transformándolo en una secuencia de inicio de trama. A continuación, agrega la información a transmitir a esta trama y la envía al anillo, por el que gira hasta que llega a la estación destino.

Mientras la trama de información gira alrededor del anillo no hay ningún otro token en la red, por lo que ninguna otra máquina puede realizar transmisiones.

Cuando la trama llega a la máquina destino, ésta copia la información contenida en ella para su procesamiento y elimina la trama, con lo que la estación emisora puede verificar si la trama se recibió y se copió en el destino.

Como consecuencia de este método determinista de transmisión, en las redes Token Ring no se producen colisiones, a diferencia de las redes CSMA/CD como Ethernet. Además, en las redes Token Ring se puede calcular el tiempo máximo que transcurrirá antes de que cualquier máquina pueda realizar una transmisión, lo que hace que sean ideales para las aplicaciones en

las que cualquier demora deba ser predecible y en las que el funcionamiento sólido de la red sea importante.

La primera red Token Ring fue desarrollada por la empresa IBM en los años setenta, todavía sigue usándose y fue la base para la especificación IEEE 802.5 (método de acceso Token Ring), prácticamente idéntica y absolutamente compatible con ella. Actualmente, el término Token Ring se refiere tanto a la red Token Ring de IBM como a la especificación 802.5 del IEEE.

Las redes Token Ring soportan entre 72 y 260 estaciones a velocidades de 4 a 16 Mbps, se implementan mediante cableado de par trenzado, con blindaje o sin él, y utilizan una señalización de banda base con codificación diferencial de Manchester.

**Tokens**

Los tokens están formados por un byte delimitador de inicio, un byte de control de acceso y un byte delimitador de fin. Por lo tanto, tienen una longitud de 3 bytes.

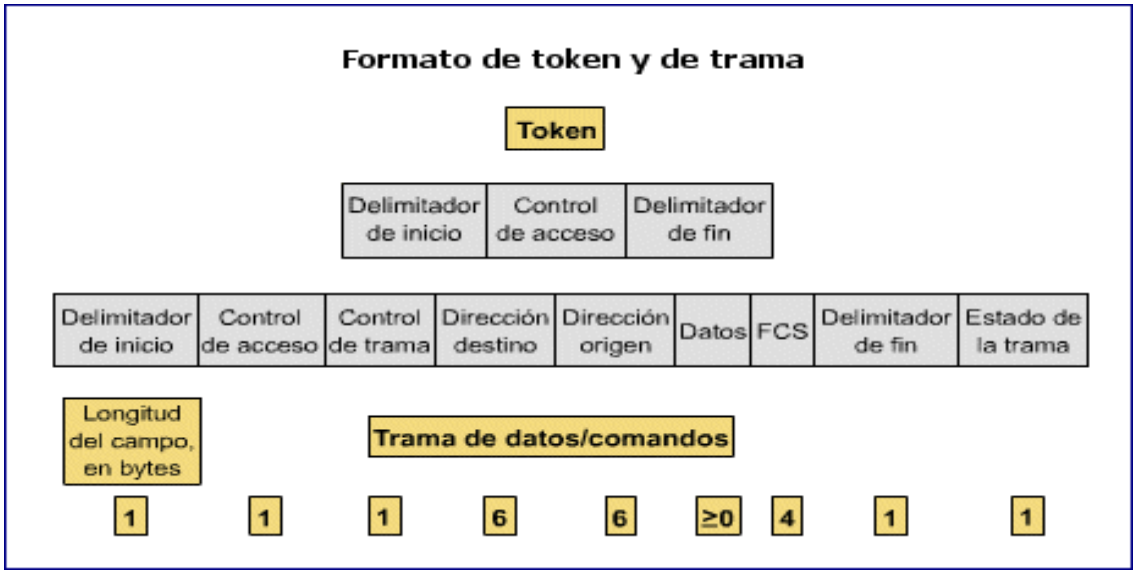



Figura Nº 07 Formato y Trama Token ring

- El delimitador de inicio alerta a cada estación ante la llegada de un token o de una trama de datos/comandos. Este campo también incluye señales que distinguen al byte del resto de la trama al violar el esquema de codificación que se usa en otras partes de la trama.
- El byte de control de acceso contiene los campos de prioridad y de reserva, así como un bit de token y uno de monitor. El bit de token distingue un token de una trama de datos/comandos y un bit de monitor determina si una trama gira continuamente alrededor del anillo.
- El delimitador de fin señala el fin del token o de una trama de datos/comandos. Contiene bits que indican si hay una trama defectuosa y una trama que es la última de una secuencia lógica.

El tamaño de las tramas de datos/comandos varía según el tamaño del campo de información. Las tramas de datos transportan información para los protocolos de capa superior, mientras que las tramas de comandos contienen información de control y no poseen datos para los protocolos de capa superior.

En las tramas de datos o instrucciones hay un byte de control de trama a continuación del byte de control de acceso. El byte de control de trama indica si la trama contiene datos o información de control. En las tramas de control, este byte especifica el tipo de información de control.

A continuación del byte de control de trama hay dos campos de dirección que identifican las estaciones destino y origen. Como en el caso de IEEE 802.5, la longitud de las direcciones es de 6 bytes. El campo de datos está ubicado a continuación del campo de dirección. La longitud de este campo está

limitada por el token de anillo que mantiene el tiempo, definiendo de este modo el tiempo máximo durante el cual una estación puede retener al token.

Y a continuación del campo de datos se ubica el campo de secuencia de verificación de trama (FCS). La estación origen completa este campo con un valor calculado según el contenido de la trama. La estación destino vuelve a calcular el valor para determinar si la trama se ha dañado mientras estaba en tránsito. Si la trama está dañada se descarta. Como en el caso del token, el delimitador de fin completa la trama de datos/comandos.

**Sistema de prioridad**

Las redes Token Ring usan un sistema de prioridad sofisticado que permite que determinadas estaciones de alta prioridad usen la red con mayor frecuencia. Las tramas Token Ring tienen dos campos que controlan la prioridad: **el campo de prioridad** y el **campo de reserva**.

Sólo las estaciones cuya prioridad es igual o superior al valor de prioridad que posee el token pueden tomar ese token. Una vez que se ha tomado el token y éste se ha convertido en una trama de información, sólo las estaciones cuyo valor de prioridad es superior al de la estación transmisora pueden reservar el token para el siguiente paso en la red. El siguiente token generado incluye la mayor prioridad de la estación que realiza la reserva. Las estaciones que elevan el nivel de prioridad de un token deben restablecer la prioridad anterior una vez que se ha completado la transmisión.

**Mecanismos de control**

Las redes Token Ring usan varios mecanismos para detectar y compensar los fallos de la red. Uno de estos mecanismos consiste en seleccionar una estación de la red Token Ring como el monitor activo. Esta estación actúa como una fuente centralizada de información de temporización para otras estaciones del anillo y ejecuta varias funciones de mantenimiento del anillo. Potencialmente cualquier estación de la red puede ser la estación de monitor activo.

Una de las funciones de esta estación es la de eliminar del anillo las tramas que circulan continuamente. Cuando un dispositivo transmisor falla, su trama puede seguir circulando en el anillo e impedir que otras estaciones transmitan sus propias tramas; esto puede bloquear la red. El monitor activo puede detectar estas tramas, eliminarlas del anillo y generar un nuevo token.

La topología en estrella de la red Token Ring de IBM también contribuye a la confiabilidad general de la red. Las **MSAU** (unidades de acceso de estación múltiple) activas pueden ver toda la información de una red Token Ring, lo que les permite verificar si existen problemas y, de ser necesario, eliminar estaciones del anillo de forma selectiva.

Otro mecanismo de control de fallos de red es el conocido como **Beaconing**. Cuando una estación detecta la existencia de un problema grave en la red (por ejemplo, un cable roto), envía una **trama de beacon**. La trama de beacon define un dominio de error. Un dominio de error incluye la estación que informa acerca del error, su vecino corriente arriba activo más cercano (NAUN) y todo lo que se encuentra entre ellos.

Entones el beaconing inicia un proceso denominado **auto-reconfiguración**, en el que los nodos situados dentro del dominio de error automáticamente ejecutan diagnósticos. Este es un intento de reconfigurar la red alrededor de las áreas en las que hay errores. Físicamente, las MSAU pueden lograrlo a través de la reconfiguración eléctrica.

#### 2.2.3.4. Redes LAN FDDI

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

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

El tráfico de cada anillo viaja en direcciones opuestas. Físicamente, los anillos están compuestos por dos o más conexiones punto a punto entre estaciones adyacentes. Los dos anillos de FDDI se conocen con el nombre de primario y secundario. El anillo primario se usa para la transmisión de datos, mientras que el anillo secundario se usa generalmente como respaldo.

Se distinguen en una red FDDI dos tipos de estaciones: las estaciones **Clase B, o estaciones de una conexión (SAS)**, se conectan a un anillo, mientras que las de **Clase A, o estaciones de doble conexión (DAS)**, se conectan a ambos anillos.

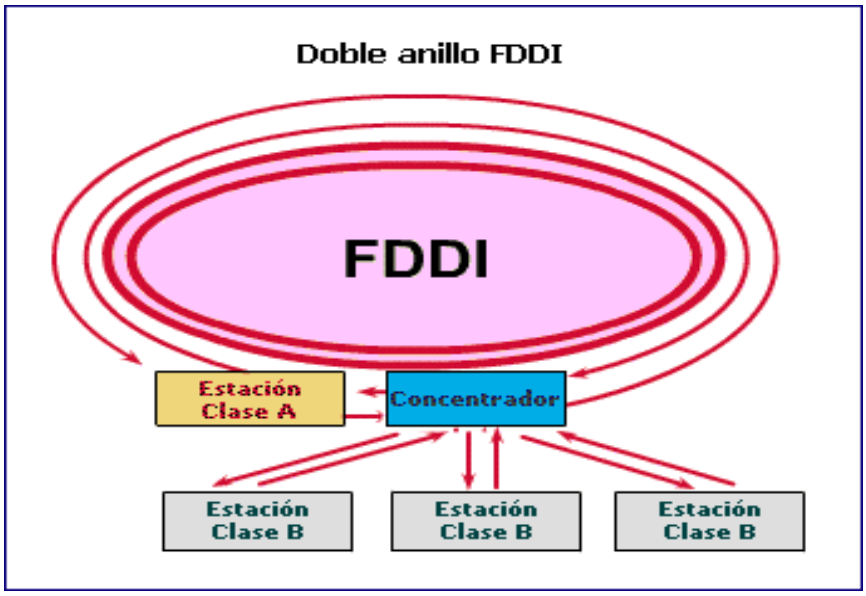



Figura Nº 08 Transmisión – Red FFDI

Las SAS se conectan al anillo primario a través de un concentrador que suministra conexiones para varias SAS. El concentrador garantiza que si se produce una falla o interrupción en el suministro de alimentación en algún SAS determinado, el anillo no se interrumpa. Esto es particularmente útil cuando se conectan al anillo PC o dispositivos similares que se encienden y se apagan con frecuencia.

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

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

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

FDDI también permite diálogos extendidos, en los cuales las estaciones pueden usar temporalmente todo el ancho de banda asíncrono.

El mecanismo de prioridad de la FDDI puede bloquear las estaciones que no pueden usar el ancho de banda síncrono y que tienen una prioridad asíncrona demasiado baja.

En cuanto a la codificación, FDDI no usa el sistema de Manchester, sino que implementa un esquema de codificación denominado **esquema 4B/5B**, en el que se usan 5 bits para codificar 4. Por lo tanto, dieciséis combinaciones son datos, mientras que las otras son para control.

Debido a la longitud potencial del amillo, una estación puede generar una nueva trama inmediatamente después de transmitir otra, en vez de esperar su vuelta, por lo que puede darse el caso de que en el anillo haya varias tramas a la vez.

Las fuentes de señales de los transceptores de FDDI son LEDs (diodos electroluminiscentes) o láser. Los primeros se suelen usar para tendidos entre

máquinas, mientras que los segundos se usan para tendidos primarios de backbone.

**Tramas FDDI**

Las tramas en la tecnología FDDI poseen una estructura particular. Cada trama se compone de los siguientes campos:

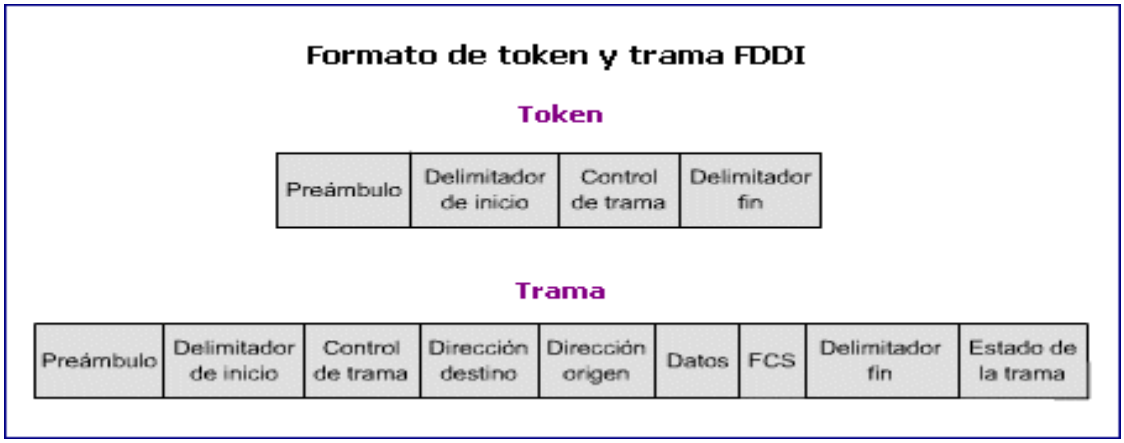



Figura Nº 09 Formato y Trama FFDI

- Preámbulo, que prepara cada estación para recibir la trama entrante.
- Delimitador de inicio, que indica el comienzo de una trama, y está formado por patrones de señalización que lo distinguen del resto de la trama.
- Control de trama, que contiene el tamaño de los campos de dirección, si la trama contiene datos asíncronos o síncronos y otra información de control.
- Dirección destino, que contiene la dirección física (6 bytes) de la máquina destino, pudiendo ser una dirección unicast (singular), multicast (grupal) o broadcast (cada estación).

- Dirección origen, que contiene la dirección física (6 bytes) de la máquina que envió la trama.
- Secuencia de verificación de trama (FCS), campo que completa la estación origen con una verificación por redundancia cíclica calculada (CRC), cuyo valor depende del contenido de la trama. La estación destino vuelve a calcular el valor para determinar si la trama se ha dañado durante el tránsito. La trama se descarta si está dañada.
- Delimitador de fin, que contiene símbolos que indican el fin de la trama.
- Estado de la trama, que permite que la estación origen determine si se ha producido un error y si la estación receptora reconoció y copió la trama.

**Medios en las redes FDDI**

FDDI especifica una LAN de dos anillos de 100 Mbps con transmisión de tokens, que usa un medio de transmisión de fibra óptica.

Aunque funciona a velocidades más altas, FDDI es similar a Token Ring. Ambas configuraciones de red comparten ciertas características, tales como su topología (anillo) y su método de acceso al medio (transferencia de tokens).

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

- Seguridad: la fibra no emite señales eléctricas que se pueden interceptar.
- Confiabilidad: la fibra es inmune a la interferencia eléctrica.

- Velocidad: la fibra óptica tiene un potencial de rendimiento mucho mayor que el del cable de cobre.

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

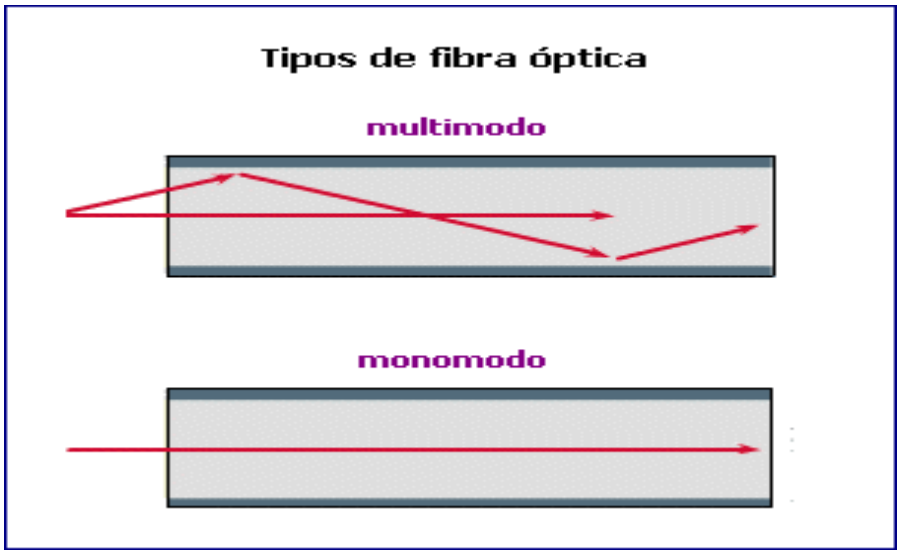



Figura Nº 10 Tipos de Fibra Óptica

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

La fibra monomodo puede acomodar un mayor ancho de banda y permite el tendido de cables de mayor longitud que la fibra multimodo. Debido a

estas características, la fibra monomodo se usa a menudo para la conectividad entre edificios mientras que la fibra multimodo se usa con mayor frecuencia para la conectividad dentro de un edificio. La fibra multimodo usa los LED como dispositivos generadores de luz, mientras que la fibra monomodo generalmente usa láser.

### 2.2.4. Redes de Área Metropolitana – MAN

Una Red de Área Metropolitana o MAN (*Metropolitan Area Network*) es básicamente una extensión más grande que una LAN y normalmente se basa en una tecnología similar. Podría abarcar un grupo de oficinas corporativas cercanas o una ciudad y podría ser privada o pública.

### 2.2.5. Redes de Área Amplia – WAN

Una Red de Área Amplia o WAN (*Wide Area Network*), se extiende sobre un área geográfica extensa, a veces un país o un continente. Contiene una colección de máquinas dedicadas a ejecutar programas de usuario (es decir, de aplicación).

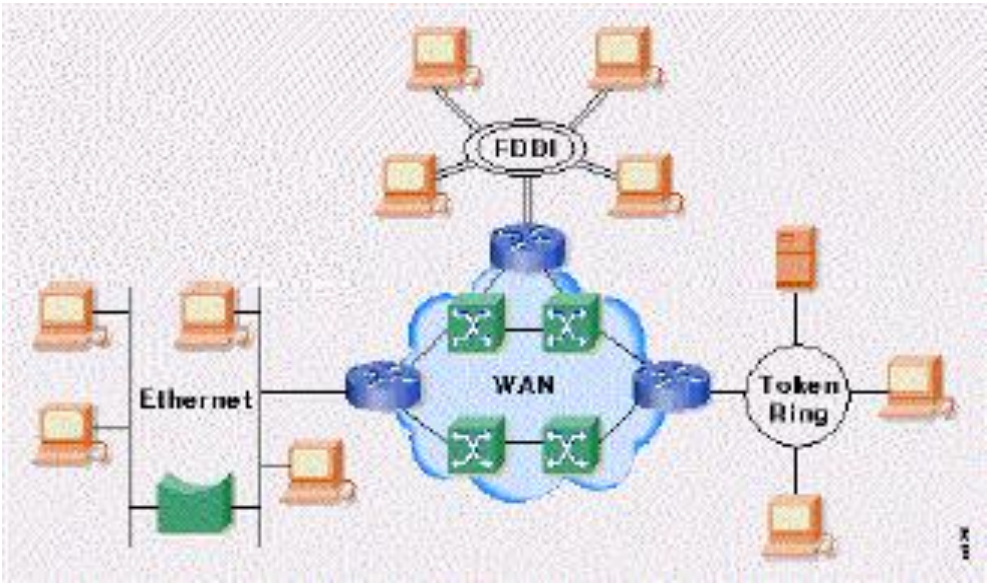


Figura Nº 11 Redes LAN – MAN - WAN

### 2.2.6. Redes Inalámbricas

Se utilizan ondas de radio o infrarrojos para llevar la información de un punto a otro sin necesidad de un medio físico. Las ondas de radio son normalmente referidas a portadoras de radio ya que éstas únicamente realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponer a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final. Esto es llamado modulación de la portadora por la información que está siendo transmitida. De este modo la señal ocupa más ancho de banda que una sola frecuencia. Varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas, si las ondas son transmitidas a distintas frecuencias de radio. Para extraer los datos el receptor se sitúa en una determinada frecuencia ignorando el resto. En una configuración típica de LAN sin cable los puntos de acceso (transceiver) conectan la red cableada de un lugar fijo mediante cableado normalizado. EL punto de acceso recibe la información, la almacena y transmite entre WLAN y LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.

El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, vía una antena.

La naturaleza de la conexión sin cable es transparente al sistema del cliente.

**Beneficios**

Utilizando una WLAN se puede acceder a información compartida sin necesidad de buscar un lugar para conectar el computador, y los administradores de la red pueden poner a punto o aumentar la red sin instalar o mover cables. Veamos más ampliamente sus beneficios.

**Visión general de los beneficios de una WLAN**

Frente a las redes tradicionales se tienen las siguientes ventajas en cuanto a productividad, comodidad y costos:

- **Movilidad:** Información en tiempo real en cualquier lugar de la organización o empresa para todo usuario de la red. El que se obtenga en tiempo real supone mayor productividad y posibilidades de servicio.
- **Facilidad de instalación:** Evita obras para tirar cable por muros y techos.
- **Flexibilidad:** Permite llegar donde el cable no puede.
- **Reducción de costos:** Cuando se dan cambios frecuentes o el entorno es muy dinámico el costo inicialmente más alto de la red sin cable es significativamente más bajo, además de tener mayor tiempo de vida y menor gasto de instalación.
- **Escalabilidad:** El cambio de topología de red es sencillo y trata igual pequeña y grande redes.

**WLAN en la Industria**

**Corporaciones:** Con WLAN los empleados pueden beneficiarse de una red móvil para el correo electrónico, compartición de archivos, y visualización de web's, independientemente de dónde se ubiquen en la oficina.

**Educación:** Las instituciones académicas que soportan este tipo de conexión móvil permiten a los usuarios con computadoras de ordenador conectarse a la red de la universidad para intercambio de opiniones en las clases, para acceso a internet, etc.

**Finanzas:** Mediante una PC portátil y un adaptador a la red WLAN, los representantes pueden recibir información desde una base de datos en tiempo real y mejorar la velocidad y calidad de los negocios. Los grupos de auditorias contables incrementan su productividad con una rápida puesta a punto de una red.

**Cuidado de la salud:** WLAN permite obtener información en tiempo real, por lo que proporciona un incremento de la productividad y calidad del cuidado del paciente eliminando el retardo en el tratamiento del paciente, los papeles redundantes, los posibles errores de trascripción, etc.

**Restaurantes y venta al por menor:** Los servicios de restaurantes pueden utilizar WLAN para directamente entrar y enviar los pedidos de comida a la mesa. En los almacenes de ventas al por menor un WLAN se puede usar para actualizar temporalmente registros para eventos especiales.

**Manufacturación:** WLAN ayuda al enlace entre las estaciones de trabajo de los pisos de la fábrica con los dispositivos de adquisición de datos de la red de la compañía.

**Almacenes:** En los almacenes, terminales de datos con lectores de código de barras y enlaces con redes WLAN, son usados para introducir datos y mantener la posición de las paletas y cajas. WLAN mejora el seguimiento del inventario y reduce los costos del escrutinio de un inventario físico.

Son varios los factores a considerar a la hora de comprar un sistema inalámbrico para la instalación de una red LAN. Algunos de los aspectos a tener en cuenta son los siguientes:

**Cobertura**

La distancia que pueden alcanzar las ondas de Radiofrecuencia (RF) o de infrarrojos (IR) es función del diseño del producto y del camino de propagación, especialmente en lugares cerrados. Las interacciones con objetos, paredes, metales, e incluso la gente, afectan a la propagación de la energía. Los objetos sólidos bloquean las señales de infrarrojos, esto impone límites adicionales. La mayor parte de los sistemas de redes inalámbricas usan RF porque pueden penetrar la mayor parte de lugares cerrados y obstáculos. El rango de cobertura de una LAN inalámbrica típica va de 30 m. a 100 m. Puede extenderse y tener posibilidad de alto grado de libertad y movilidad utilizando puntos de acceso (micro células) que permiten "navegar" por la LAN.

**Rendimiento**

Depende de la puesta a punto de los productos así como del número de usuarios, de los factores de propagación (cobertura, diversos caminos de propagación), y del tipo de sistema inalámbrico utilizado. Igualmente depende

del retardo y de los cuellos de botella de la parte cableada de la red. Para la más comercial de las redes inalámbricas los datos que se tienen hablan de un rango de 1.6 Mbps Los usuarios de Ethernet o Token Ring no experimentan generalmente gran diferencia en el funcionamiento cuando utilizan una red inalámbrica. Estas proporcionan suficiente rendimiento para las aplicaciones más comunes de una LAN en un puesto de trabajo, incluyendo correo electrónico, acceso a periféricos compartidos, acceso a Internet, y acceso a bases de datos y aplicaciones multiusuario. Como punto de comparación una LAN inalámbrica operando a 1.6 Mbps es al menos 30 veces más rápida.

**Integridad y fiabilidad**

Estas tecnologías para redes inalámbricas se han probado durante más de 50 años en sistemas comerciales y militares. Aunque las interferencias de radio pueden degradar el rendimiento éstas son raras en el lugar de trabajo. Los robustos diseños de las testeadas tecnologías para LAN inalámbricas y la limitada distancia que recorren las señales, proporciona conexiones que son mucho más robustas que las conexiones de teléfonos móviles y proporcionan integridad de datos de igual manera o mejor que una red cableada.

**Compatibilidad con redes existentes**

La mayor parte de LANS inalámbricas proporcionan un estándar de interconexión con redes cableadas como Ethernet o Token Ring. Los nodos de la red inalámbrica son soportados por el sistema de la red de la misma manera que cualquier otro nodo de una red LAN, aunque con los discos apropiados.

Una vez instalado, la red trata los nodos inalámbricos igual que cualquier otro componente de la red.

**Interoperatividad de los dispositivos inalámbricos dentro de la red**

Los consumidores deben ser conscientes de que los sistemas inalámbricos de redes LAN de distintos vendedores pueden no ser compatibles para operar juntos. Tres razones:

- Diferentes tecnologías no interoperarán. Un sistema basado en la tecnología de Frecuencia Esperada (FHSS), no se comunicará con otro basado en la Tecnología de Secuencia Directa (DSSS).
- Sistemas que utilizan distinta banda de frecuencias no podrán comunicar aunque utilicen la misma tecnología.
- Aún utilizando igual tecnología y banda de frecuencias ambos vendedores, los sistemas de cada uno no comunicarán debido a diferencias de implementación de cada fabricante.

**Interferencia y Coexistencia**

La naturaleza en que se basan las redes inalámbricas implica que cualquier otro producto que transmita energía a la misma frecuencia puede potencialmente dar cierto grado de interferencia en un sistema LAN inalámbrico. Por ejemplo los hornos de microondas, pero la mayor parte de fabricantes diseñan sus productos teniendo en cuenta las interferencias por Microondas. Otro problema es la colocación de varias redes inalámbricas en lugares próximos. Mientras unas redes inalámbricas de unos fabricantes interfieren con otras redes inalámbricas, hay otras redes que coexisten sin

interferencia. Este asunto debe tratarse directamente con los vendedores del producto.

### Licencias

En los Estados Unidos, La Comisión Federal de Comunicaciones (FCC), gobierna la radio-transmisión, incluida la empleada en las redes inalámbricas. Otras naciones tienen sus correspondientes agencias reguladoras. Típicamente las redes inalámbricas se diseñan para operar en porciones del espectro de radio donde el usuario final no necesita una licencia FCC para utilizar las ondas de radio. En los Estados Unidos la mayor parte de las redes difunden en una de las bandas de ISM (de instrumentación, científicas o médicas). Estas incluyen 902 - 928 MHz, 2.4 - 2.483 GHz, 5.15 - 5.35 GHz, y 5.725 - 5.875 GHz Para poder vender productos de sistemas de LAN inalámbricos en un país en particular, el fabricante debe asegurar la certificación por la agencia encargada en ese país.

### Simplicidad y Facilidad de Uso

Los usuarios necesitan muy poca información a añadir a la que ya tienen sobre redes LAN en general, para utilizar una LAN inalámbrica. Esto es así porque la naturaleza inalámbrica de la red es transparente al usuario, las aplicaciones trabajan de igual manera que lo hacían en una red cableada, Los productos de una LAN inalámbrica incorporan herramientas de diagnóstico para dirigir los problemas asociados a los elementos inalámbricos del sistema. Sin embargo, los productos están diseñados para que los usuarios rara vez tengan que utilizarlos.

Las LAN inalámbricas simplifican muchos de los problemas de instalación y configuración que atormentan a los que dirigen la red. Ya que únicamente los puntos de acceso de las redes inalámbricas necesitan cable, ya no es necesario llevar cable hasta el usuario final. La falta de cable hace también que los cambios, extensiones y desplazamientos sean operaciones triviales en una red inalámbrica. Finalmente, la naturaleza potable de las redes inalámbricas permite a los encargados de la red pre configurar ésta y resolver problemas antes de su instalación en un lugar remoto. Una vez configurada la red puede llevarse de un lugar a otro con muy poca o ninguna modificación.

**Seguridad en la Comunicación**

Puesto que la tecnología inalámbrica se ha desarrollado en aplicaciones militares, la seguridad ha sido uno de los criterios de diseño para los dispositivos inalámbricos. Normalmente se suministran elementos de seguridad dentro de la LAN inalámbrica, haciendo que estas sean más seguras que la mayor parte de redes cableadas. Es muy complicado que los receptores no sintonizados escuchar el tráfico que se da en la LAN.

Complejas técnicas de encriptado hacen imposible para todos, incluso los más sofisticados, acceder de forma no autorizada al tráfico de la red. En general los nodos individuales deben tener habilitada la seguridad antes de poder participar en el tráfico de la red.

**Escalabilidad**

Las redes WLAN pueden ser diseñadas para ser extremadamente simples bastante complejas. WLAN's pueden soportar un amplio número de

nodos y/o extensas áreas físicas añadiendo puntos de acceso para dar energía a la señal o para extender la cobertura.

**Alimentación en las plataformas móviles**

Los productos WLAN de los usuarios finales están diseñados para funcionar sin corriente alterna o batería de alimentación proveniente de sus portátiles, puesto que no tienen conexión propia cableada. Los fabricante se emplean técnicas especiales para maximizar el uso de la energía del computador y el tiempo de vida de su batería.

**Observaciones de WLAN**

El IEEE 802.11 define opciones de la capa física para la transmisión inalámbrica y la capa de protocolos MAC. El IEEE 802.11 representa el primer estándar para los productos WLAN de una internacionalmente conocida organización independiente.

## 2.3. TOPOLOGIA DE RED

Con topología se entiende la configuración espacial de los cables que componen el sistema de cableado.

Es necesario precisar que la topología física puede ser en algunos casos diferente de la lógica, es decir del modo en que la señal alcanza los varios usuarios de la red.

### 2.3.1. Topología en bus

En la topología en bus, la red está formada por un único cable que se articula a lo largo de la ruta.

Al cable de red se conectan los distintos usuarios mediante una interfaz. La sencillez de esta conexión choca con algunas contradicciones. En especial, es intuitivo comprender cómo al cortar el cable principal corresponda la interrupción de todo el servicio de red.

Además existen normas que limitan la extensión de los cables principales y de las conexiones usuario denominados cables “drop”) que convierten estas soluciones escasamente utilizables en el presente.

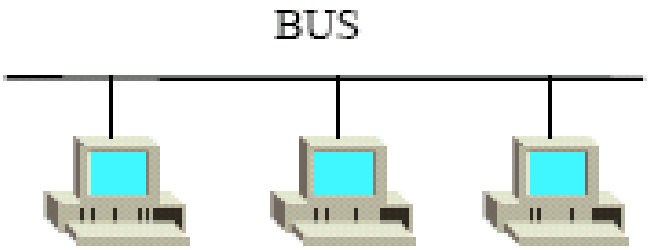



Figura Nº 12 Topología BUS

### 2.3.2. Topología en estrella

En la topología en estrella, los cables convergen hacia un punto de concentración principal que normalmente coincide con la posición en donde está el equipo al cual se debe llevar la conexión.

Las ventajas de un cableado con la topología en estrella se identifican fácilmente: mayor capacidad de configuración del sistema, gracias a la

presencia de un punto principal de administración que recoge las terminaciones de todos los cables y una mayor inmunidad contra las fallas (a cada cable se conecta sólo un usuario).

La desventaja es naturalmente el mayor costo ya que es necesario prever un cable para cada punto de uso del sistema y adecuadas canalizaciones para tender los cables en todos los puntos del edificio. Es la que se sigue en la mayoría de las ocasiones.

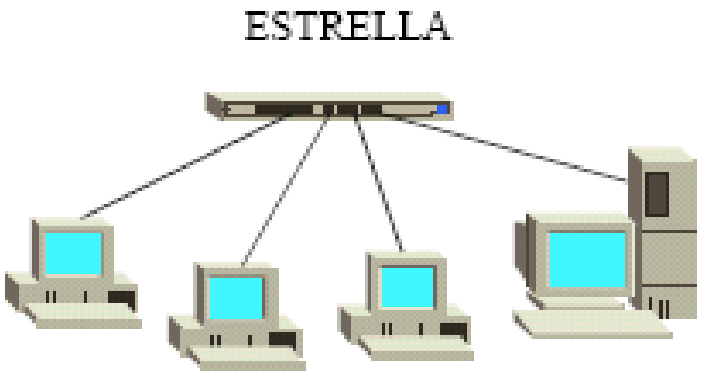



Figura Nº 13  Topología ESTRELLA

### 2.3.3. Topología en anillo

En la topología en anillo, cada usuario se conecta a la máquina que lo antecede y a la siguiente en un anillo cerrado.

En una red en anillo, los datos se mueven en una única dirección a lo largo de la red hasta alcanzar el usuario destinatario o regresar a donde se ha originado la señal.

También en este caso la interrupción del anillo debería en práctica producir la caída de la red.

Sin embargo, es posible observar cómo la primera aplicación que aprovecha esta configuración (red Token Ring) haya solucionado este problema.

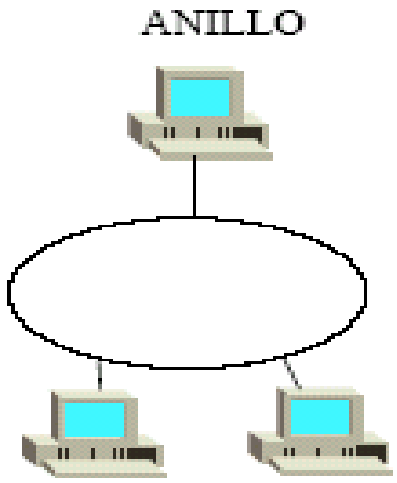



Figura Nº 14  Topología ANILLO

## 2.4 MODELO DE REFERENCIA

Existen dos arquitecturas de red importantes: el modelo de referencia OSI y el modelo de referencia TCP/IP.

### 2.4.1 El Modelo de Referencia OSI

El modelo OSI se muestra en la figura 2.1 (menos el medio físico). Este modelo se basa en una propuesta que desarrolló la Organización Internacional de Normas (ISO, por sus siglas en inglés) como primer paso hacia la estandarización internacional de los protocolos que se usan en las diversas capas. El modelo se llama **modelo de referencia OSI** (*Open Systems Interconnection*, **interconexión de sistemas abiertos**) de la ISO puesto que

se ocupa de la conexión de sistemas abiertos, esto es, sistemas que están abiertos a la comunicación con otros sistemas.

### Capa Física

La **capa física** tiene que ver con la transmisión de bits por un canal de comunicación. Las consideraciones de diseño tienen que ver con la acción de asegurarse de que cuando un lado envíe un bit 1, se reciba en el otro lado como un bit 1, no como un bit 0. Aquí las consideraciones de diseño tienen mucho que ver con las interfaces mecánica, eléctrica y de procedimientos, y con el medio de transmisión físico que está bajo la capa física.

### Capa de Enlace de Datos

La tarea principal de la **capa de enlace de datos** es tomar un medio de transmisión en bruto y transformarlo en una línea que parezca libre de errores de transmisión. Esta tarea la cumple al hacer que el emisor divida los datos de entrada en **tramas de datos** (unos cientos o miles de bytes, normalmente), que transmita las tramas en forma secuencial y procese las **tramas de acuse de recibo** que devuelve el receptor. Puesto que la capa física sólo acepta y transmite una corriente de bits sin preocuparse por su significado o su estructura, corresponde a la capa de enlace de datos crear y reconocer los límites de las tramas. Esto se puede lograr añadiendo patrones especiales de bits al principio y al final de las tramas. Si estos patrones de bits ocurrieran en los datos por accidente, se debe tener cuidado especial para asegurar que estos patrones no se interpreten incorrectamente como delimitadores de trama.

Una ráfaga de ruido en la línea puede destruir por completo una trama. En este caso, el *software* de la capa de enlace de datos de la máquina fuente puede retransmitir la trama. Sin embargo, las transmisiones repetidas de la misma trama introducen la posibilidad de duplicar tramas. Se podría enviar una trama duplicada si se perdiera la trama de acuse de recibo que el receptor devuelve al emisor. Corresponde a esta capa resolver el problema provocado por las tramas dañadas, perdidas y duplicadas. La capa de enlace de datos puede ofrecer varias clases de servicio distintas a la capa de red, cada una con diferente calidad y precio.

Otra consideración que surge en la capa de enlace de datos (y también en la mayor parte de las capas más altas) es cómo evitar que un transmisor veloz sature de datos a un receptor lento. Se debe emplear algún mecanismo de regulación de tráfico para que el transmisor sepa cuánto espacio de almacenamiento temporal (*buffers*) tiene el receptor en ese momento.

Si se puede usar la línea para transmitir datos en ambas direcciones, esto introduce una nueva complicación que el *software* de la capa de enlace de datos debe considerar. El problema es que las tramas de acuse de recibo para el tráfico de A a B compiten por el uso de la línea con tramas de datos para el tráfico de B a A.

Las redes de difusión tienen una consideración adicional en la capa de enlace de datos: cómo controlar el acceso al canal compartido. Una subcapa especial de la capa de enlace de datos se encarga de este problema, la subcapa de acceso al medio.

**Capa de Red**

La **capa de red** se ocupa de controlar el funcionamiento de la subred. Una consideración clave de diseño es determinar cómo se encaminan los mensajes (llamados aquí **paquetes**) de la fuente a su destino. La rutas se pueden basar en tablas estáticas que se “alambran” en la red y rara vez se cambian. También se pueden determinar al inicio de cada conversación. Por último, pueden ser altamente dinámicas, determinándose de nuevo con cada paquete para reflejar la carga actual de la red.

Si en la subred se encuentran presentes demasiados paquetes a la vez, se estorbarán mutuamente, formando cuellos de botella. El control de tal congestión pertenece también a la capa de red.

En vista de que los operadores de la subred podrían esperar remuneración por su labor, con frecuencia hay una función de contabilidad integrada en la capad de red.

Cuando un paquete debe viajar de una red a otra para alcanzar su destino, pueden surgir muchos problemas. El tipo de direcciones que usa la segunda red puede ser diferente del de la primera; puede ser que la segunda no acepte en absoluto el paquete por ser demasiado grande; los protocolos pueden diferir y otras cosas. La capa de red debe resolver todos estos problemas para lograr que se interconecten redes heterogéneas.

En las redes de difusión el problema del ruteo es simple y la capa de red con frecuencia es delgada o incluso inexistente.

**Capa de Transporte**

La función básica de la **capa de transporte** es aceptar datos de la capa de sesión, dividirlos en unidades más pequeñas si es necesario, pasarlos a la capa de red y asegurar que todos los pedazos lleguen correctamente al otro extremo. Además, todo esto se debe hacer de manera eficiente y en forma que aísle a las capas superiores de los cambios inevitables en la tecnología del *hardware*.

En condiciones normales, la capa de transporte crea una conexión de red distinta para cada conexión de transporte que requiera la capa de sesión. Sin embargo, si la conexión de transporte requiere un volumen de transmisión alto, la capa de transporte podría crear múltiples conexiones de red, dividiendo los datos entre las conexiones para aumentar el volumen. Por otro lado, si es costoso crear o mantener una conexión de red, la capa de transporte puede multiplexar varias conexiones de transporte en la misma conexión de red para reducir el costo.

En todos los casos, la capa de transporte debe lograr que la multiplexión sea transparente para la capa de sesión.

La capa de transporte determina también qué tipo de servicio proporcionará a la capa de sesión y, finalmente, a los usuarios de la red. El tipo de servicio se determina al establecer la sesión.

La capa de transporte es una verdadera capa de extremo a extremo, del origen al destino.

En otras palabras, un programa en la máquina fuente sostiene una conversación con un programa similar en la máquina destino, haciendo uso de

los encabezados de mensajes y de los mensajes de control. En las capas bajas, los protocolos se usan entre cada máquina y sus vecinas inmediatas, y no entre las máquinas de origen y destino, que pueden estar separadas por muchos enrutadores. La diferencia entre las tres primeras capas, que están encadenadas, y las restantes, que son extremo a extremo. Muchos nodos están multiprogramados, lo que implica que múltiples conexiones entran y salen de cada nodo.

En este caso se necesita una manera de saber cuál mensaje pertenece a cuál conexión. El encabezado de transporte (H4), es una opción para colocar esta información.

Además de multiplexar varias corrientes de mensajes por un canal, la capa de transporte debe cuidar de establecer y liberar conexiones a través de la red. Esto requiere alguna clase de mecanismo de asignación de nombres, de modo que un proceso en una máquina pueda describir con quién quiere conversar. También debe haber un mecanismo para regular el flujo de información, a fin de que un nodo rápido no pueda saturar a otro lento. Tal mecanismo se llama **control de flujo** y desempeña un papel clave en la capa de transporte (también en otras capas). El control de flujo entre nodos es distinto del control de flujo entre enrutadores, aunque se aplican principios similares a ambos.

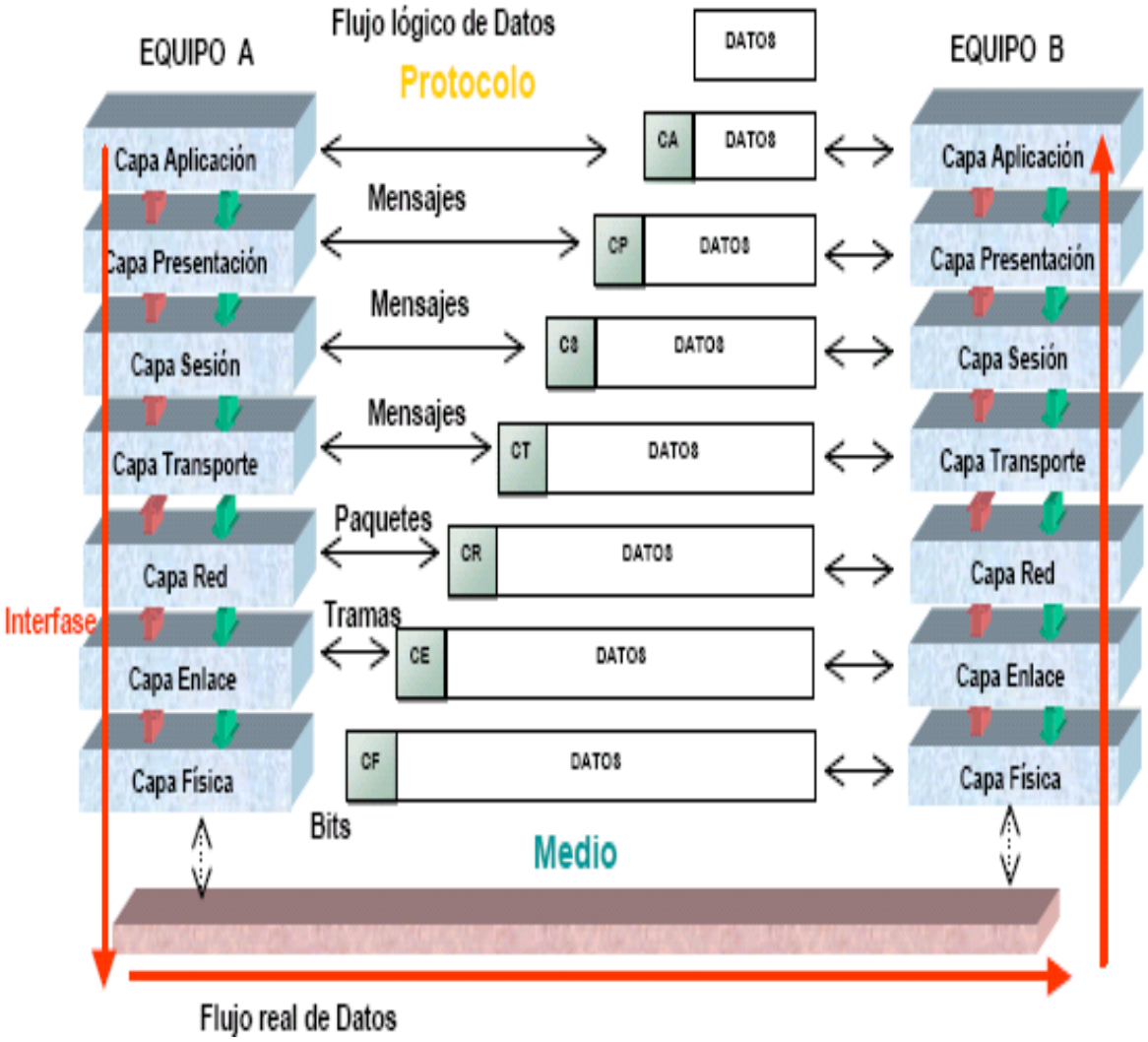



Figura Nº 15 Modelo de Referencia OSI (Transmisión)

El modelo OSI tiene siete capas. Los principios que se aplicaron para llegar a las siete capas son los siguientes:

Se debe crear una capa siempre que se necesite un nivel diferente de abstracción.

Cada capa debe realizar una función bien definida.

La función de cada capa se debe elegir pensando en la definición de protocolos estandarizados internacionalmente.

Los límites de las capas deben elegirse a modo de minimizar el flujo de información a través de las interfaces.

La cantidad de capas debe ser suficiente para no tener que agrupar funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se vuelva inmanejable.

El modelo de OSI en sí no es una arquitectura de red porque no especifica los servicios y protocolos exactos que se han de usar en cada capa; sólo dice lo que debe hacer cada capa.

Sin embargo, la ISO también ha elaborado estándares para todas las capas, aunque no sean parte del modelo de referencia mismo. Cada uno se ha publicado por separado como norma internacional.

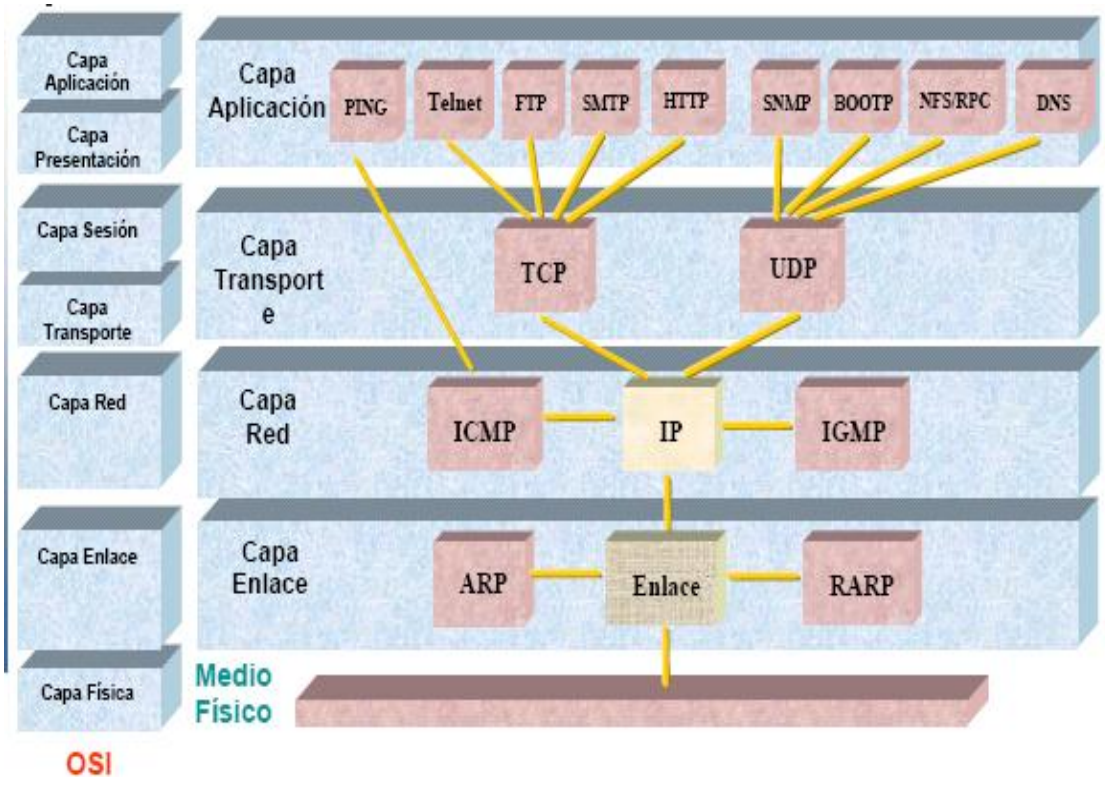



Figura Nº 16 Aplicaciones del Modelo de Referencia OSI

### 2.4.2 El Modelo de Referencia TCP/IP

Este modelo es el empleado en Internet. Así, la capacidad de conectar entre sí múltiples redes de manera inconsútil fue uno de los principales objetivos de diseño desde el principio. Esta arquitectura se popularizó después como el **modelo de referencia TCP/IP**, por las iniciales de sus dos protocolos primarios.

En este modelo se pretendía que las conexiones permanecieran intactas mientras las máquinas de origen y destino estuvieran funcionando, aun si alguna de las máquinas o de las líneas de transmisión en el trayecto dejara de funcionar de forma repentina. Es más, se necesitaba una arquitectura flexible, pues se tenía la visión de aplicaciones con requerimientos divergentes.

#### Capa de InterRed

Todos estos requerimientos condujeron a la elección de una red de conmutación de paquetes basada en una capa de interred carente de conexiones. Esta capa, llamada **capa de interred**, es el eje que mantiene unida toda la arquitectura. La misión de esta capa es permitir que los nodos inyecten paquetes en cualquier red y los hagan viajar de forma independiente a su destino (que podría estar en otra red diferente). Los paquetes pueden llegar incluso en un orden diferente a aquel en que fueron enviados, en cuyo caso corresponde a las capas superiores reacomodarlos, si se desea la entrega ordenada.

La capa de interred define un formato de paquete y protocolo oficial llamado **IP** (*Internet Protocol*, **protocolo de interred**). El trabajo de la capa

interred es entregar paquetes IP a donde se supone que deben ir. Aquí la consideración más importante es claramente el ruteo de los paquetes, y también evitar la congestión. Por lo anterior es razonable decir que la capa de interred TCP/IP es muy parecida en funcionalidad a la capa de red OSI.

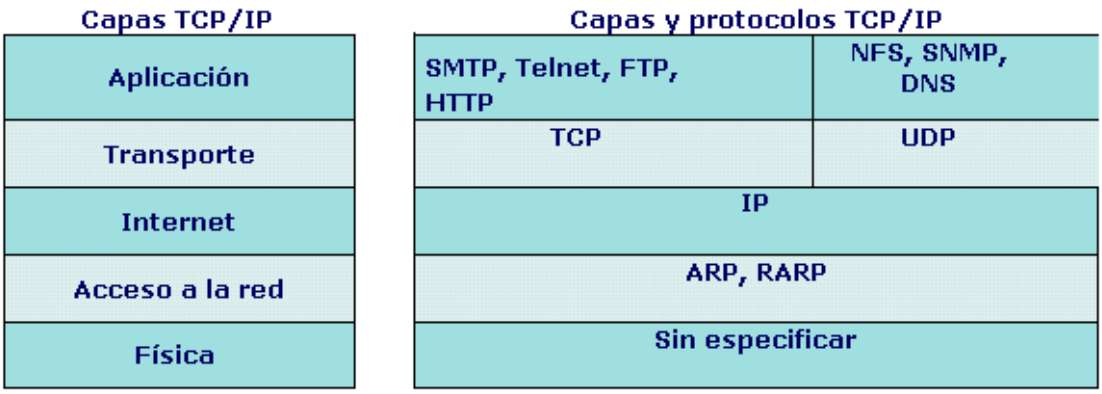



Figura Nº 17 Modelo de Referencia TCP / IP y Aplicaciones

**Capa de Transporte**

La capa que está sobre la capa de interred en el modelo TCP/IP se llama usualmente ahora **capa de transporte**. Esta capa se diseñó para permitir que las entidades pares en los nodos de origen y destino lleven a cabo una conversación, lo mismo que en la capa de transporte OSI. Aquí se definen dos protocolos extremos a extremo. El primero, **TCP** (*Transmisión Control Protocol*, **protocolo de control de transmisión**) es un protocolo confiable orientado a la conexión que permite que una corriente de bytes originada en una máquina se entregue sin errores en cualquier otra máquina de la interred. Este protocolo fragmenta la corriente entrante de bytes en mensajes discretos y pasa cada uno a la capa de interred. En el destino, el receptor reensambla los mensajes recibidos para formar la corriente de salida. El TCP también se encarga del

control de flujo para asegurar que un emisor rápido no pueda abrumar a un receptor lento con más mensajes de los que pueda manejar. El segundo protocolo de esta capa, el **UDP** (*User Datagram Protocol*, **protocolo de datagrama de usuario**), es un protocolo sin conexión, no confiable, para aplicaciones que no necesitan la asignación de secuencia ni de control de flujo del TCP y que desean utilizar los suyos propios. Este protocolo también se usa ampliamente para consultas de petición y respuesta de una sola ocasión, del tipo cliente servidor, y en aplicaciones en las que la entrega pronta es más importante que la entrega precisa.

**Capa de Aplicación**

El modelo TCP/IP no tiene capa de sesión ni de presentación. La experiencia con el modelo OSI ha comprobado que esta visión fue correcta: se utilizan muy poco en la mayor parte de las aplicaciones.

Encima de la capa de transporte está la **capa de aplicación**, que contiene todos los protocolos de alto nivel. Entre los protocolos más antiguos están el de terminal virtual (TELNET) y el de transferencia de archivos (FTP), el de correo electrónico (SMTP); aunque en la actualidad existen muchos más.

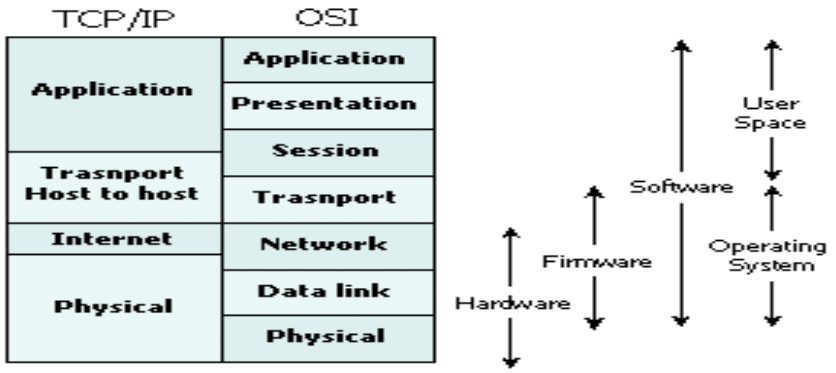



Figura Nº 18 Comparación del los Modelos de Referencia OSI TPC/IP

## 2.5 SEGURIDAD DE ACCESO A INTERNET

Esta parte está dedicada al caso en el que se desee dar acceso a Internet a un conjunto de ordenadores. Esta situación puede darse en el caso de una empresa u organización que quiere conectar a sus empleados a Internet o en el caso de que se desee montar un proveedor de servicios de Internet (ISP).

Ahora es necesario distinguir entre los diferentes mecanismos que pueden ofrecerse para conseguir esta protección: filtros de paquetes, "TCP wrappers", etc.

Cabe destacar que todo lo dicho para el caso de acceso de ordenadores individuales a Internet, sigue siendo válido para este caso más general. Por un lado todos los ordenadores a los que se de acceso a Internet podrían aplicar los mecanismos descritos en el apartado anterior para controlar individualmente su seguridad. Por otro el sistema que sirva de punto de acceso podrá aplicar esas mismas técnicas o similares para protegerse a si mismo y ofrecer una protección global a la red interna.

La principal diferencia es que ahora la preocupación no es por un ordenador individual sino por toda una red. Por ejemplo, en el caso de un virus de mail el objetivo será evitar que llegue a ninguno de los ordenadores de la red a la que se da acceso. Si bien, cabe la posibilidad de proteger individualmente cada uno de los ordenadores es mucho más eficiente (en tiempo y dinero) solucionarlo de forma general para todos, instalando las herramientas adecuadas en los sistemas a través de los que accede toda la red.

También adquieren importancia algunas nuevas amenazas que no eran necesarios considerar en el caso de acceso con un ordenador individual.

Algunas de ellas se describen a continuación:

Un caso que se da con excesiva frecuencia ocurre cuando los usuarios de una red local usan las posibilidades que ofrecen sus sistemas operativos para compartir ficheros. Si en un momento dado la red local se conecta a Internet los usuarios pueden no ser conscientes de que están compartiendo sus ficheros con cualquier ordenador conectado a Internet. Esta es una amenaza de acceso no autorizado a información y esta información puede ir desde claves de acceso, información personal (económica por ejemplo), datos confidenciales de la empresa, etc. El asunto se agrava por el hecho de que aunque una persona de la red local tenga cuidado con su información compartida es posible que otra a la que le pasa esta información no haya tenido cuidado y al final una persona no autorizada puede acceder a ella.

Además de las amenazas pueden citarse otras dos que pueden tener bastante gravedad:

Ataques que impidan la conexión a Internet. Este es un tipo de ataque de Denegación de Servicio.

Intrusión en el sistema que sirve de punto de acceso. Esta es una amenaza muy grave dado que una vez en este sistema el atacante puede acceder con mucha mayor facilidad a cualquier ordenador de la red local.

**Sistemas de Cortafuegos**

En la parte anterior ya se comenzó el tratamiento de los sistemas de cortafuegos. Sin embargo entonces el tratamiento era desde el punto de vista del uso que podía darle un individuo para proteger su ordenador conectado a Internet.

Ahora se profundizará en estas herramientas para abarcar el caso de unos cortafuegos que se sitúa entre Internet y una red local a la que debe proteger.

Podemos clasificar los cortafuegos en dos tipos genéricos:

**Filtros de paquetes ("packet filters")**

En los que se controla el envío, recepción y retransmisión de los paquetes TCP/IP que atraviesan el cortafuegos. Dentro de este tipo se encontrarían los filtros de paquete con inspección de estados que incorporarían el conocimiento del estado de las comunicaciones al filtrado de éstas.

**Pasarelas de aplicación ("application proxies")**

En este esquema la comunicación no se realiza nunca directamente contra la aplicación (servidor web, correo electrónico, etc.) La conexión del sistema remoto se realiza contra la pasarela instalada en los cortafuegos. Esta comprueba la operación que se desea realizar sobre la aplicación, permitiendo de esta forma un control del origen, destino y contenido de la comunicación.

Envoltorios TCP (TCP Wrappers)

Estos filtros se sitúan entre la red y cada una de las aplicaciones que escuchan peticiones de la red. Se denominan así porque se sitúan al nivel del protocolo de transporte de Internet, TCP.

En los sistemas UNIX, y GNU/Linux no es una excepción, el filtro TCP más utilizado es tcpd de Wietse Venema. Esa herramienta permite especificar desde que ordenadores se podrá conectar y desde cuales no a cada uno de los servicios de nuestro ordenador.

Lo más habitual es pensar que un ordenador de usuario final no tiene ningún servicio y por tanto esta protección no es necesaria, pero esto no es así. Como se ha dicho, por defecto hay diversos servicios de red activados. E incluso aunque se desactiven, en todo sistema operativo de red hay aplicaciones que 'abren' servicios para sus propios propósitos.

La configuración de tcpd es muy sencilla y por ello no existe ninguna herramienta específica para realizarla. Se basa en dos archivos, /etc/hosts.allow y /etc/hosts.deny donde se especifica desde donde se permite y desde donde no se permite respectivamente acceder a cada servicio. Además, estas definiciones pueden ser comprobadas con las herramientas tcpdchk y tcpmatch para verificar los posibles casos de uso.

Uno de los puntos débiles de tcpd y sus herramientas auxiliares es la falta de una herramienta de configuración de fácil uso y que integre todas las posibilidades que ésta ofrece. Sin embargo, con la importancia creciente que se está dando a este aspecto dentro del mundo del software libre es posible que aparezca alguna pronto.

Filtros de paquetes

Un filtro de paquetes puede admitir, rechazar o simplemente descartar los paquetes que le llegan con destino a unas redes internas o salientes desde ésta. Estas decisiones se toman en función de una serie de reglas establecidas por el administrador. Estas reglas pueden basarse, en principio, en la siguiente información contenida en un paquete:

Direcciones origen y destino.

Puertos TCP origen y destino.

Protocolo empleado.

Una generación posterior de los cortafuegos de filtrado de paquetes puede incorporar una tecnología conocida como "inspección de estados" que permite validad los paquetes en función del estado de la conexión. Es decir, los paquetes TCP podrán rechazarse si no siguen el protocolo establecido ("three-way handshake"), por ejemplo, si se envía un paquete FIN sin haber establecido una comunicación previamente. Igualmente, acercándose cada vez más a los cortafuegos de pasarela de aplicación, se podrá limitar una comunicación a nivel de aplicación si no sigue el protocolo correcto, por ejemplo, el envío de un LS en una comunicación FTP sin haber realizado previamente la autenticación con el comando USER.

GNU/Linux (y también las distintas versiones de BSD) disponen de sistemas de filtrado de paquetes integrados en el propio sistema operativo. Esta integración ofrece una gran fiabilidad a este filtrado, ya que pasa siempre por el núcleo del sistema operativo antes de llegar a ninguna aplicación en el espacio de usuarios.

Este soporte de filtrado de paquetes viene dado por:

ipfwadm

Es la versión usada por las versiones antiguas de GNU/Linux.

**ipchains**

Es usado por las versiones de GNU/Linux 2.2. Contiene mejoras significativas como la posibilidad de crear grupos de reglas arbitrarios. Es decir no se limita al administrador a los típicos "input", "output" y "forward".

**iptables (netfilter)**

Es la nueva versión incluida (y escrita completamente desde cero) en la última serie del kernel de GNU/Linux, la 2.4. Contiene varias novedades muy interesantes. La más importante de ellas es que se implementa mecanismos de inspección de estados.

También se han hecho grandes mejoras en su gestión, que ahora es a la vez más fácil y potente. A pesar de ello iptables es compatible con versiones anteriores.

***SINUS***

Es una alternativa independiente a las opciones anteriores. Es un producto bastante completo que se distribuye bajo la licencia GPL y que dispone de documentación bastante buena y herramientas de configuración propias.

El soporte de filtrado viene acompañado de una interfaz de administración de línea de comandos, pero además existen un número interesante de aplicaciones (gráficas en su mayoría) que facilitan su gestión. Generalmente estas aplicaciones funcionan para más de una herramientas

listadas antes. Algunas de estas, pensadas para usuarios finales sin conocimientos profundos de seguridad han sido descritas en la sección anterior. Las herramientas que aquí se indican siguen siendo de gran ayuda para el administrador de red que tiene que configurar unos cortafuegos por cuanto permiten una configuración más versátil de las reglas de este tipo de cortafuegos.

Generalmente el cortafuego se sitúa en el sistema que actúa de encaminador y que de todas formas es necesario, así que no es imprescindible incorporar hardware extra a la arquitectura de conexión.

**gfcc**

Permite configurar reglas de ipchains e ipfwadm de forma gráfica pero dejando al administrador el mismo control que la herramienta de línea de comandos. Para usar esta herramienta es necesario conocer la filosofía de funcionamiento de ipchains o ipfwadm.

**ipmenu**

Es una interfaz de usuario basada en la librería ncurses. En otras palabras es una interfaz textual basada en menús. A pesar de no ser gráfico es fácil de usar a la vez que potente en flexible. Está pensado para configurar iptables y permite desde una única interfaz configurar el filtrado y modificación de paquetes, la traducción de direcciones (NAT) y las características de encaminamiento (iproute2).

A continuación se muestra una captura de ipmenu. En ella se puede apreciar la gran potencia de esta herramienta.

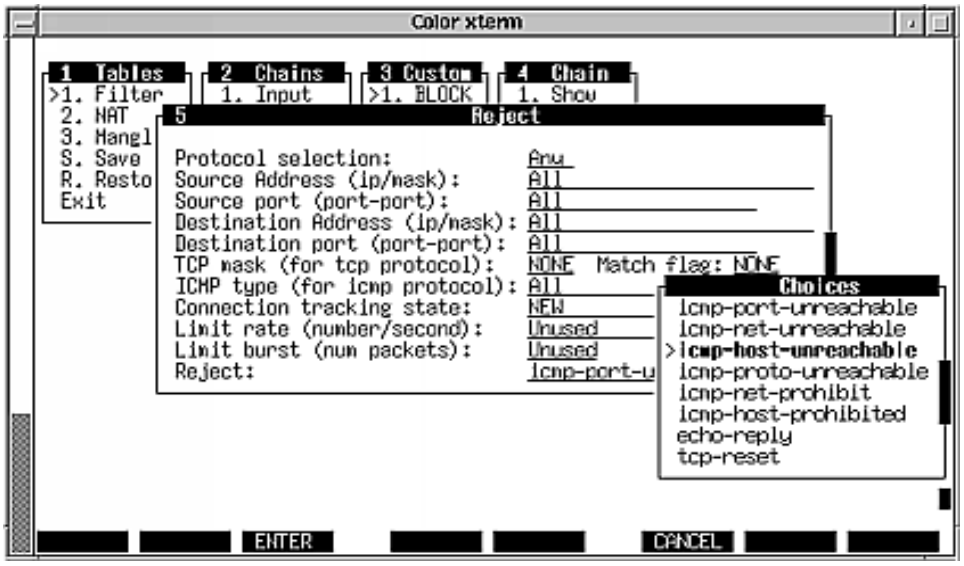



Figura Nº19 Uno de los Menús de ipmenu

**Easyfw**

Esta es una herramienta gráfica bastante fácil de usar. Tras establecer la dirección de la interfaz interna y la dirección de la interfaz externa se pasa a configurar de forma independiente reglas para los paquetes entrantes (input rules), salientes (output rules) o que van a ser reenviados (forwarding rules).

Además dispone de la funcionalidad adicional de permitir almacenar varias configuraciones e incluso añadir comentarios a cada una para identificarlas fácilmente.

Easyfw incluye soporte para GNU/Linux únicamente, en concreto para ipfwadm e ipchains.

A continuación se incluye una captura de pantalla de la herramienta.

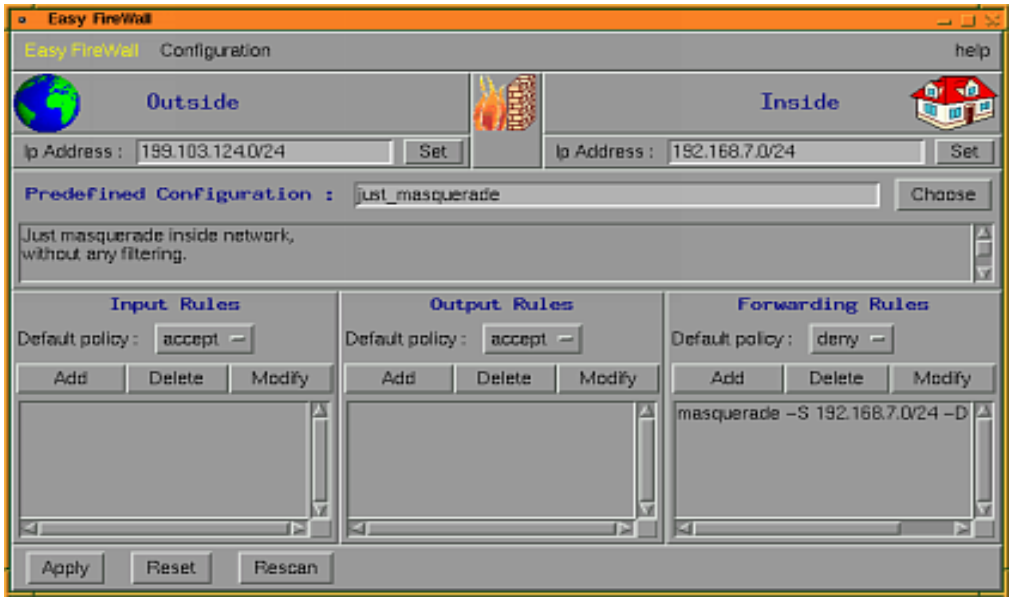



Figura Nº20 Pantalla Principal de easyfw

**Knetfilter**

Es una interfaz interfaz de usuario de configuración de cortafuegos para el escritorio KDE. Es muy completo permitiendo realizar configuraciones comunes rápidamente a la vez que configuraciones más complejas y personalizadas.

Una característica muy interesante es su posible integración con tcpdump para examinar los paquetes que transcurren por la red y con nmap para realizar un escaneo para comprobar la fiabilidad de los cortafuegos una vez configurado. Más adelante se describirán con más detalle estas herramientas.

Cabe notar que knetfilter sólo se encuentra disponible para la versión 2.4 de Linux.


Figura Nº 21 Ventanas de knetfilter durante configuración contra fuegos

**FERM**

Esta es una herramienta de ayuda a los administradores que tienen que mantener cortafuegos muy complejos. FERM permite almacenar todas las reglas en un fichero y cargarlo empleando un comando. Este fichero de configuración tiene una sintaxis similar a un lenguaje de programación partiendo crear listas y agrupación por niveles de las reglas. FERM se distribuye bajo la licencia GPL.

Mason

Ofrece una forma de configuración de cortafuegos de una forma enormemente original. Básicamente permite configurar unos cortafuegos aprendiendo a partir de tráfico real generado en la red donde se desea que actúe los cortafuegos.

**PHP firewall generator**

Esta herramienta está pensada para ser instalado en un ordenador propio con soporte para PHP (ver glosario). Se accede a ella a través de un navegador y mediante una serie de formularios se configuran directamente las reglas de filtrado del cortafuegos. Esta aplicación se distribuye bajo licencia GPL y está alojado en SourceForge.

A continuación se muestra una captura bastante completa que incluye la ventana principal y dos ventanas auxiliares, una con una lista de reglas (abajo) y otra editando una de estas reglas (arriba a la derecha).

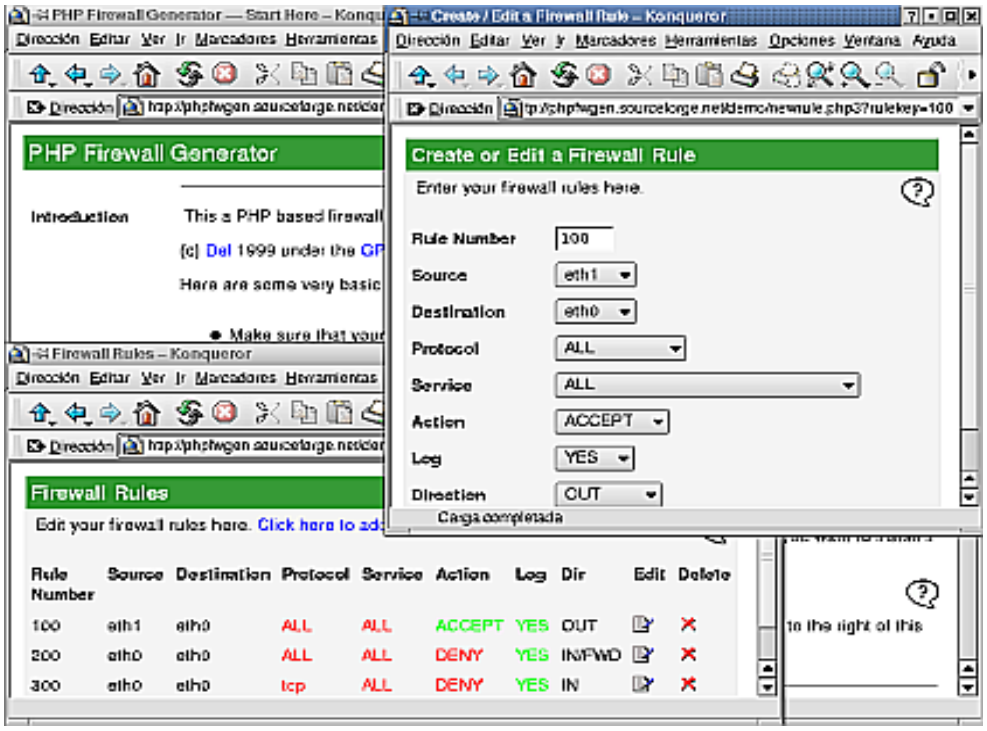



Figura Nº 22 Ventanas configurando un cortafuegos con PHP Firewall Generator

Una última opción interesante es Firewall configuration toolkit (TCP) que puede obtenerse en fct.linuxfirewall.org . Una vez instalado puede configurarse

un cortafuego rellenando información sobre la política de seguridad deseada a través de una interfaz web.

### Cortafuegos propietarios

Una alternativa propietaria a los cortafuegos libres presentados es Firewall-1 de Check Point. Este es uno de los cortafuegos líderes del mercado, junto con el módulo de cortafuegos PIX de **CISCO**. Las capacidades de ambos son, en principio, similares a los productos presentados previamente aunque dirigidos a una solución completa que integra muchas otras funciones que las que se podrían, en principio, atribuir a un cortafuegos de filtrado. En el caso de Firewall-1, dispone de un software de gestión y monitorización del cortafuegos (que en los productos de software libre son funciones separadas debido a la habitual arquitectura modular de UNIX), generación de redes privadas virtuales (VPN), integración con software de alta disponibilidad, y capacidades de filtrado de URLs y código malicioso, del que carecen en principio, las tecnologías anteriores (aunque pueda ser un componente proporcionado por otros proyectos de software libre su integración no es inmediata).

### Pasarelas de aplicación ("PROXIES")

Este tipo de herramientas se instalan en sistemas intermedios entre los ordenadores finales de la red interna e Internet. Cuando se desea conectar con el exterior se debe hacer a través de la pasarela, que será la que realmente se comunicará con los ordenadores externos. Cuando reciba una respuesta de estos la reenviará al ordenador interno que inició la conexión. La forma de hacer esto es específica de cada aplicación y por tanto sólo podrá usarse la

pasarela con aquellas aplicaciones específicamente soportadas por esta. Las aplicaciones más usuales como la navegación por el web (HTTP) o el correo electrónico están soportadas por un gran número de pasarelas.

La gran ventaja de este esquema es que se tiene un control global sobre la seguridad y además este control se tiene a nivel individual sobre cada una de las aplicaciones. Esto permite comprender y mantener el estado en el que se encuentra una comunicación y con ello reconocer y evitar un mayor número de ataques.

Pero las pasarelas de aplicación también tienen inconvenientes. Una de ellas es precisamente que requiere una configuración específica para cada uno de los usos que se van a hacer de la red: HTTP, FTP, telnet, correo, news, etc. Además las aplicaciones finales de los usuarios deben estar preparadas para usar la pasarela como sistema intermedio para llegar a un destino. Afinando un poco más, en realidad esta última afirmación no es del todo cierta. Últimamente han aparecido las pasarelas transparentes que con algo de ayuda del sistema operativo permiten que las aplicaciones no tengan que ser modificadas.

En este tipo de cortafuegos, las implementaciones propietarias son múltiples destacando Gauntlet Firewall de PGP, y Raptor Eagle de Axent. Estos cortafuegos incorporan generalmente capacidades mixtas de proxy y de cortafuegos de filtrado (aunque no estén diseñados específicamente para esta función), pudiéndose establecer reglas de filtrado, de traducción de direcciones, redirección de puertos. De igual forma, dado que se hace una inspección de los contenidos, pueden integrarse con otras soluciones para categorización y filtrado de URLs, análisis de código malicioso, capacidades de antivirus, etc. Existe, por ejemplo, una plataforma de e-ppliance de la compañía Nokia

basada en Gauntlet para ofrecer una solución antivirus de **caja negra**. En cualquier caso, es habitual encontrar en estos cortafuegos propietarios capacidades de establecimiento de redes privadas virtuales y de alta disponibilidad. Aunque ésta última característica aún está poco desarrollada en las implementaciones propietarias de estos cortafuegos.

Las implementaciones de tecnología proxy, en el campo de software libre, están, sin embargo, muy retrasadas frente a las implementaciones propietarias. En el caso del cortafuegos Gauntlet, se disponen de proxies a nivel de aplicación para más de treinta servicios distintos (desde http hasta bases de datos Oracle, servicios de X, whois, finger, correo, etc). Existen proxies disponibles en software libre para los servicios de http, DNS, X, correo, FTP e IRC, pero no existe un paquete integrado que los ofrezca todos de forma conjunta con una interfaz de administración única. Además, las capacidades de control de estos proxies están lejos de igualarse a las ofrecidas por los cortafuegos de proxy propietarios.

# CAPITULO III

## 3.1 ANÁLISIS DE LA PROBLEMÁTICA

El presente estudio, plantea alternativas para un servicio de comunicaciones en las instalaciones del Hospital de Apoyo “JAMO” en la ciudad de Tumbes, la cual sea capaz de integrar los servicios de Voz, Datos y Video.

Se evaluó la situación actual de los sistemas de comunicación del Hospital de Apoyo “JAMO”, teniendo en observación la forma de enlace, medios de comunicación y tipo de distribución de la red.

Se realizo la toma de datos mediante un catastro de todos los equipos de comunicación y computo en los distintos servicios del hospital.

## 3.2 ESTADO ACTUAL DE LA RED DE COMUNICACIONES

Se detalla en el presente estudio las posibilidades de desarrollar un buen servicio de los sistemas de telefonía, datos y video.

### 3.2.1 Sistema Telefónico

En la actualidad el sistema telefónico no existe como debería de ser en las instalaciones del Hospital de Apoyo “JAMO”.

Teniendo varias líneas telefónicas independientes para determinados servicios dentro de las instalaciones.

Debemos recalcar que la cantidad de líneas telefónicas independientes como de equipos celulares, es debido a la deficiente y falta de equipos como una central telefónica, siendo los equipos celulares uso exclusivo de personal administrativos de la institución. Ver Figura Nº 2

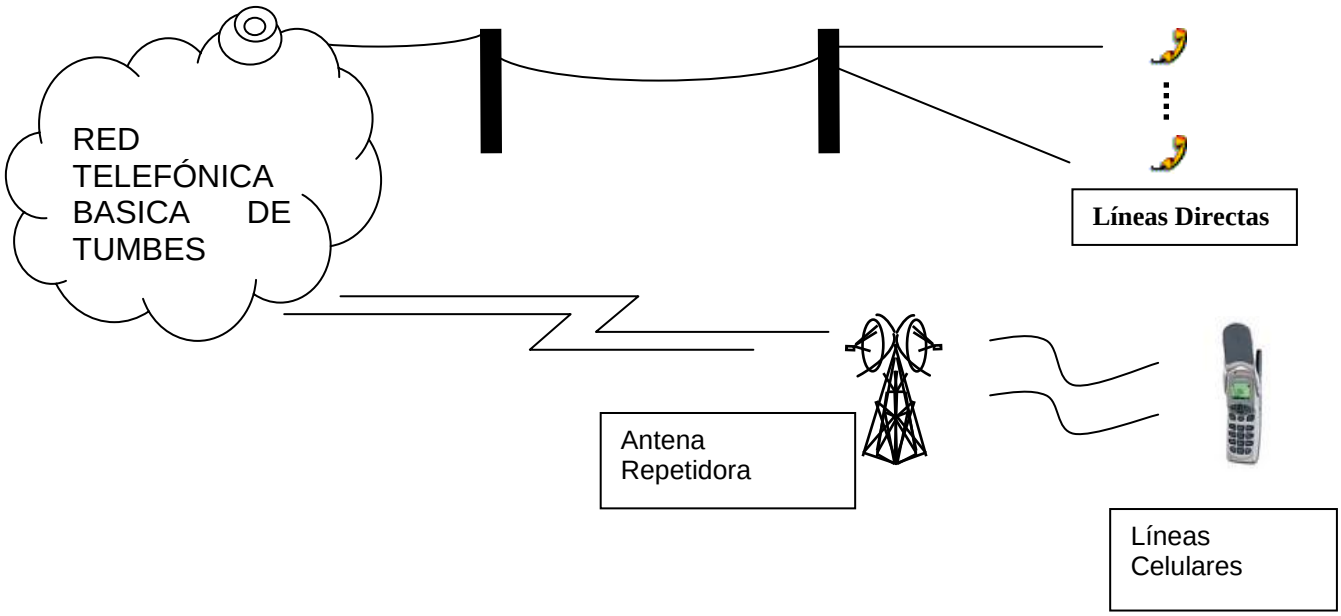



***Figura Nº 23 Sistema de Telefónico del Hospital de Apoyo "JAMO"***

### 3.2.2 Sistema de Datos

El sistema de comunicación de datos, es básico y pequeño, presenta dos redes pequeñas y aisladas de si mismas, ya que una tiene que ver con el Sistema Integrado de Administración Financiera - SIAF del Ministerio de Economía y Finanzas (Oficina de Economía y Finanzas) la cual conectada a través de una línea dedicada vía telefónica enlaza a cuatro computadoras de otros servicios administrativos por intermedio de un Switch (Ver Figura Nº 3), la otra es exclusiva para el Sistema Integral de Salud (SIS) también por línea dedicada enlazada a cuatro computadoras mediante un Hub (Ver Figura Nº 4). Actualmente se cuenta con un Centro de Gestión de Red (inicialmente en formación) que cuenta con un Sistema Sppedy (Telefónica del Perú), que enlazados por un Modem - Router, a dos maquinas de ultima generación.

Teniendo en cuenta que la red debe ampliarse por que otros servicios administrativos deben usar ese mismo sistema y requieren estar interconectadas entre si para mejor el servicio.

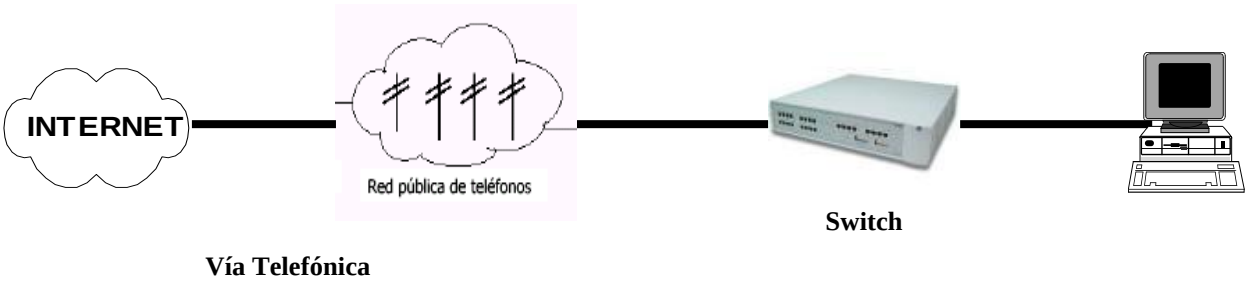



***Figura Nº 24 Sistema de Datos - SIAF***

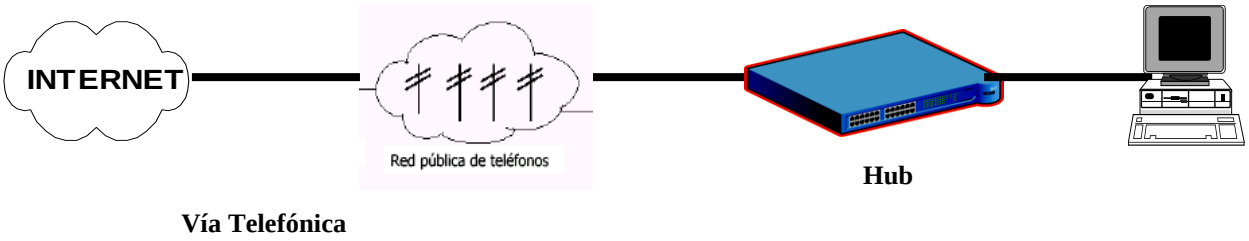



***Figura Nº 25 Sistema de Datos - SIS***

Además existen dentro de las instalaciones del hospital, un determinado numero de computadoras independientes, impresoras y otros.

Nº de Computadoras “STAND ALONE” : 35

Nº de Impresoras: 28

Nº de NIC’s: 25

Encontrándose aun computadoras con tecnología de las Pentium I y II en funcionamiento, pero la mayoría son ultimas, Pentium III y IV (Ver Tabla Nº1)

El **Centro de Gestión de Red del Hospital de Apoyo “JAMO”**, será el punto principal de la expansión de la Red de Comunicaciones Integral del

Hospital, para así brindar un mejor servicio hospitalario. Actualmente cuenta con un Modem – Router de 4 Ports Ethernet, dos Computadoras (Pentium III y IV), una Impresora LasertJet 1000 Series. El Servicio mediante la línea telefónica es de 256 Kbps. (Actualmente se encuentra como se muestra en la Figura Nº 5).

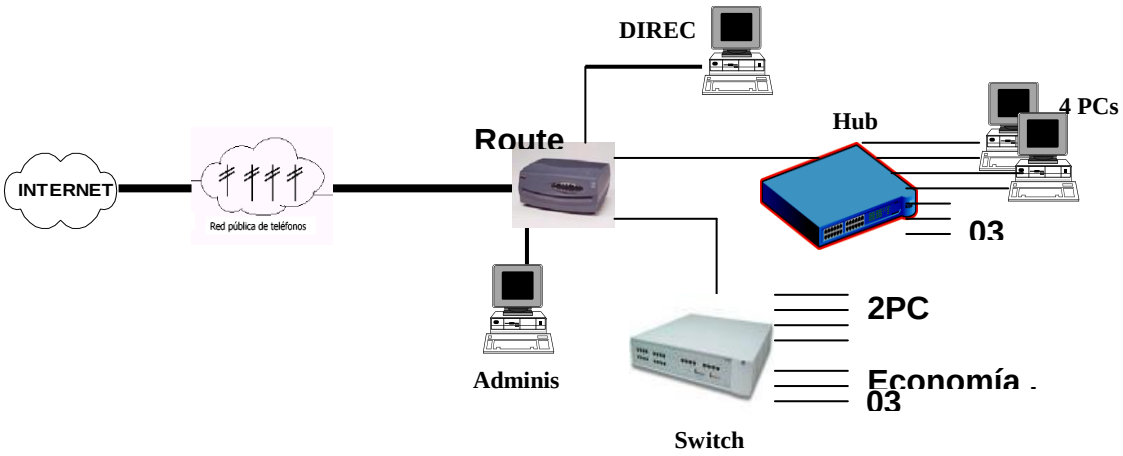



***Figura Nº 26 Sistema de Datos – Centro de Gestión Red***

## *Tabla Nº 01 Catastro de Equipos de Cómputo*

| **Oficinas** | **Pentium I** | **Pentium II** | **Pentium III** | **Pentium IV** |
|---|---|---|---|---|
| Dirección Ejecutiva | 0 | 1 | 0 | 1 |
| Dirección Administrativa | 0 | 1 | 0 | 0 |
| Oficina de Logística | 1 | 1 | 1 | 0 |
| Oficina de Presupuesto | 0 | 1 | 0 | 1 |
| Oficina de Patrimonio | 0 | 0 | 0 | 1 |
| Sistema Integral de Salud (S.I.S.) | 0 | 1 | 2 | 1 |
| Oficina de Tesorería | 0 | 0 | 1 | 0 |
| Oficina de Economía | 0 | 1 | 1 | 1 |
| Oficina de Estadística | 0 | 1 | 1 | 0 |
| Oficina Secretaría de Enfermería | 0 | 1 | 0 | 0 |
| Centro de Gestión de Red | 0 | 0 | 1 | 0 |
| Oficina de Maternidad | 0 | 1 | 0 | 0 |
| Oficina de Farmacia | 0 | 1 | 0 | 1 |
| Oficina de Personal | 0 | 1 | 1 | 0 |
| Oficina de Planificación | 0 | 0 | 1 | 0 |
| Oficina de Mantenimiento | 0 | 0 | 1 | 0 |
| Otros Servicios | 0 | 3 | 4 | 1 |
| TOTALES PARCIALES | 1 | 14 | 14 | 7 |
| TOTAL | 36 PC's | | | |

***Tabla Nº 02 Catastro de Equipos de Conmutación***

| Equipos de Red | Marca | Serie | Modelo | Nº. Ports |
|---|---|---|---|---|
| Modem Router | ZyXEL Communications Corp. | Ethernet Sw&Wireless LAN | Prestige 650HW-31 | 4 |
| Switch | 3COM | 3C16794 | Office Connect Dual Speed | 8 |
| Hub | 3COM | 4902A046 | Office Connect Dual Speed | 8 |

### 3.2.3 Sistema de Videoconferencia

El Hospital no cuenta con sistema de videoconferencia, la cual es vital para las capacitaciones y interconexión con otras entidades de salud.

## 3.3 IDENTIFICACIÓN DEL PROBLEMA

Los problemas tanto tecnológicos como económicos que presenta la institución se detalla seguidamente.

**Sistema Telefónico**

A la demanda de los sistemas telefónicos, cada oficina o servicio dentro del hospital busco su propia solución a sus necesidades respectivas.

La instalación y el tendido de los cables, desde los postes hacia las áreas administrativas o servicios, empobrecen la estética de canalización del servicio.

Estas carencias que presenta la mala instalación y descontinuado mantenimiento de las vías telefónicas, son las que exponen a las temperaturas y medios climáticos de la zona, como la de personas no especializadas perjudicando el servicio.

**Sistema de Datos**

La red de datos que cuenta actualmente el hospital son las redes aisladas que son; la línea dedicada del Sistema SIAF – MEF, así como del SIS, y el Sistema Speedy de 256Kbps, que realmente deben estar integradas para atender las necesidades del centro hospitalario.

**Sistema de Videoconferencia**

El Hospital de Apoyo "JAMO" – Tumbes, no cuenta con un servicio de videoconferencia, en sus instalaciones.

## 3.4 REQUERIMIENTOS DE LA RED DE COMUNICACIONES

Se trata individualmente los requerimientos de cada sistema, dando importancia al Sistema de Datos, por la gran demanda de cada día de personas que requirieren de los servicios hospitalarios.

Ello no quiere quitar importancia a las demás sistemas, que son vitales para el servicio de atención administrativo – hospitalario.

### 3.4.1 Servicio Telefónico

Reducir los gastos de telefonía independiente por servicio administrativo hospitalario, conectándose todos en un solo nodo a una central telefónica (PBX) de una cantidad determinada de anexos para los servicios requeridos dentro del hospital.

Se recomienda un sistema de voz basada en la tecnología RDSI, y así aprovechar el soporte para el sistema de videoconferencia.

Así mismo realizar una reinstalación del cableado telefónico en los recorridos mal instalados o cableados.

### 3.4.2 Servicio de Datos

Viendo la importancia de este servicio, se requiere lo siguiente:

- Integrar todos los sistemas de cómputo a un punto de interconexión, de una red de gestión.
- Se recomienda adquirir nuevos equipos y sistema de computo (PC's, Switches, Routers, etc.)
- El sistema de interconexión o enlace debe soportar servicios de internet, así como dar la seguridad de la información que se trate en la institución, que solo competen al desarrollo del mismo.
- Debe soportar redes virtuales (VLAN's) para asuntos de seguridad y transferencia de información clasificada de investigación e institucional.
- Se debe contar con las normas de electrificación para el desarrollo de una red integral de servicios.

***Tabla Nº 3 Equipo de Conmutación Propuestos***

| **Equipo** | **Cantidad** | **Características** |
|---|---|---|
| PC's | 34 | Pentium IV / 1,8Ghz / 512 Kbps |
| Router | 1 | Alta Calidad de Servicio / Seguridad |
| Switch | 2 | 10/100 Mbps. |

### 3.4.3 Servicio de Videoconferencia

Este servicio es una necesidad vital, para la actualización y capacitación del personal medico – hospitalario.

El equipamiento de videoconferencia deberá cumplir la recomendación H.320 (Protocolo de Comunicación Multimedia) de la UIT.

La velocidad de la línea dependerá de la calidad de imagen y voz que se requiera para el desarrollo de las actividades médicas y administrativas.

Se recomienda instalar un punto de Videoconferencia en el Auditorio del Hospital.

# CAPITULO IV

## 4.1 SISTEMAS DE CABLEADO ESTRUCTURADO

Los rápidos cambios tecnológicos de los últimos años en materia de comunicaciones hicieron indispensable la consideración del cableado en los edificios como una inversión estratégica para la adopción de nuevas tecnologías de transmisión, sin que exista la necesidad de realizar tendidos adicionales.

Tradicionalmente hemos visto que a los edificios se les ha ido dotando distintos servicios de mayor o menor nivel tecnológico. Así se les ha dotado de calefacción, aire acondicionado, suministro eléctrico, megafonía, seguridad, etc, características que no implican dificultad, y que permiten obtener un edificio automatizado.

Cuando a estos edificios se les dota de un sistema de gestión centralizado, con posibilidad de interconexión entre ellos, y se le otra de una infraestructura de comunicaciones (voz, datos, textos, imágenes), empezamos a hablar de edificios inteligentes o racionalizados.

El desarrollo actual de las comunicaciones, vídeo conferencia, telefax, servicios multimedia, redes de ordenadores, hace necesario el empleo de un sistema de cableado estructurado avanzado capaz de soportar todas las necesidades de comunicación.

Estas tecnologías se están utilizando en: Hospitales, áreas comerciales, edificios industriales, viviendas, etc.

Un sistema de cableado estructurado consiste de una arquitectura abierta, de un medio estandarizado, de interfaces de conexión estándar, del cumplimiento de estándares nacionales e internacionales y un diseño de sistema e instalación total.

Estos estándares ya establecidos y que son continuamente actualizados surgieron debido a que cada fabricante de ordenadores utilizaba tipos distintos de cables, con topología y conectores diferentes.

Esto traía como consecuencia que:

- El conocimiento de los distintos sistemas de cableado propietario estaba solo al alcance de algunos instaladores muy especializados.
- Cada vez que alguien precisaba cambiar su ordenador, incluso de la misma marca, debía deshacer el cableado existente y proceder a un nuevo cableado, cada vez con una vida más efímera.

Aunque las computadoras son un pilar fundamental para el avance y administración tanto del trabajo como de la tecnología, estás pierden su sentido si no están conectadas a algún otro equipo computacional. Al haber dos o más de estos equipos interconectados se forman una red, la cual puede crecer tanto como nuestras necesidades lo requieran.

Los sistemas de cableado estructurado nacen con el objeto de unificar y organizar los sistemas interconectados. Estos sistemas están, normalmente, constituidos por un elevado número de componentes y requieren una cuidadosa instalación para poder asegurar un óptimo rendimiento.

En efecto, cabe recodar que el problema que se debe solucionar es suministrar un medio físico de transporte para señales generadas por una computadora.

Por lo tanto, es la aplicación computacional que determina el nivel de prestaciones necesario para el sistema de conexión y, si es necesario hipotizar un futuro no bien delineado, serán probablemente los servicios disponibles para el usuario a determinar las prestaciones necesarias para el sistema informático en su conjunto.

En otras palabras, es posible considerar que el mercado de los sistemas de cableado y relativas redes evolucionará en sintonía con las exigencias impuestas por las aplicaciones (Internet, E-commerce, entretenimiento, multimedia, etc.).

La presencia de varios sistemas para la transmisión de la información, a menudo conectados por sistemas de cableado diferentes, ha creado no pocos problemas a los usuarios:

- Dificultad de gestión.
- Costos de renovación / ampliación muy elevados.
- Apiñamiento de las canalizaciones

Además, numerosos estudios han destacado la importancia fundamental que el cableado ocupa en la transmisión de datos.

Se ha demostrado, como en la mayoría de los casos, los problemas que se han encontrado en los procesos de comunicación dependen de las ineficiencias del sistema de cableado.

La contemporánea evaluación de los costos asociados a las paradas de la máquina ha impulsado a numerosos usuarios a dedicar mayor atención al modo en que los varios equipos eran conectados y a considerar el sistema de cableado como una parte integrante (y fundamental) de la infraestructura de red.

El sistema de cableado estructurado debe estar en condiciones de responder a las innumerables exigencias manifestadas por el mercado:

- Flexibilidad – posibilidad de conectar en una plataforma común aplicaciones diferentes, normalmente utilizadas con cableados específicos o patentados.
- Confiabilidad – capacidad de garantizar prestaciones óptimas y fáciles operaciones para la solución de las fallas.
- Gestionabilidad – posibilidad de efectuar reconfiguraciones, cambios y ampliaciones de manera sencilla y rápida.
- Funcionamiento económico – beneficio y protección de la inversión seguros.

Los fabricantes no han defraudado las esperanzas y desde los años ’90 el sistema de cableado estructurado ha entrado con derecho a formar parte de las infraestructuras civiles, igual que las instalaciones eléctricas o los sistemas de seguridad y supervisión.

### 4.1.1 Subsistemas de Cableado Estructurado

Realizar un cableado estructurado significa equipar un edificio con un sistema de cables y elementos de conexión que asegure la comunicación entre todos los equipos de información.

Los subconjuntos que forman un cableado estructurado en un edificio son los siguientes:

1.- Entrada de servicios

2.- Cuarto de equipo

3.- Cableado vertical o dorsal (Backbone)

4.- Armario de telecomunicaciones

5.- Cableado horizontal

6.- Área de trabajo

La estructura de este conjunto debe ser rigurosamente de tipo en estrella y organizada según niveles jerárquicos, de acuerdo con un esquema y método preestablecidos para asegurar el mantenimiento inclusive después de frecuentes operaciones de mantenimiento y ajustes.

#### 1.- Entrada de servicios

Incluye la acometida telefónica y todo lo necesario para conectar la red de área local con los servicios del exterior.

### 2.- Cuarto de equipo

Es el lugar en donde en general se concentran los equipos activos de la red compartidos por numerosos usuarios: servidores, switches, ruteadores, pero también PBX y los equipos que gestionan el tráfico telefónico.

En definitiva, el cuarto de equipos es el espacio en donde se ejecutan las operaciones ordinarias que administran la instalación y por lo tanto es el centro clave del sistema. Es de importancia vital identificar un lugar adecuado, seguro, bien iluminado y de fácil alcance para las canalizaciones de los cables.

**Principales Características**

Este cuarto debe albergar los equipos para el control climático del ambiente (en caso de computadoras de gran tamaño) y para controlar los accesos para garantizar la seguridad de los equipos contenidos. Es necesario prever un cuarto no sometido a posibles inundaciones, infiltraciones, depósito de materiales inflamables, fuentes de interferencias electromagnéticas (motores, transmisores, etc.) con espacio suficiente como para albergar todos los equipos activos, los armarios, las canaletas y los cables de montante, además de las futuras expansiones eventuales. Además el cuarto de equipos desempeña la función de punto de administración principal ya que el cableado vertical presente entre los armarios de telecomunicaciones convergen a la misma y se conectan a los servicios de entrada o a los equipos activos de la red.

### 3.- Cableado vertical, red dorsal o backbone

El subsistema de dorsal de edificio es una ruta del cable principal que lleva todas las señales desde los armarios de telecomunicaciones hasta el cuarto de equipos y debe soportar las exigencias actuales y las futuras del usuario.

El subsistema comprende:

- Rutas de cableado.
- Cables entre el cuarto de equipos y la interfaz de red.
- Cables de conexión entre un armario de telecomunicaciones y otro conectado al mismo en el mismo piso.

El cable dorsal se utiliza para conectar los paneles de parcheo de planta con el cuarto de equipos.

En fin, cabe recordar que mientras la trama de cableado horizontal es normalizado y objeto de certificación, no lo es la dorsal vertical que puede ser función de la aplicación.

Entre numerosas aplicaciones que se desean hacer, es determinante evaluar cuáles son los medios de transmisión más adecuados para la conexión de los diferentes armarios de telecomunicación. En particular, en función de la aplicación se puede utilizar para la conexión un cable de fibra óptica o un cable de cobre:

- Cables multipares no blindados de tipo UTP.
- Cable de fibra óptica multimodal.
- Cable de fibra óptica monomodo.

Para elegir el tipo de cable, es necesario considerar:

- Las distancias cubiertas entre un armario de telecomunicaciones y cuarto de equipo.
- Las rutas utilizadas que deben ser las más cortas, seguras y baratas.
- El ancho de banda que desea utilizar el cliente.
- Las futuras expansiones de la red.

### 4.- Armario de Telecomunicaciones

El armario de telecomunicaciones es la cabina técnica que contiene y protege los equipos de comunicación y de servicio. Actúa como punto de transición entre el cableado vertical de edificio y el de la distribución horizontal.

Contiene los aparatos activos, las terminaciones de los cables y agrupa los componentes que gestionan las conexiones, administrando el sistema para la planta.

Instalando el armario en zonas no dedicadas, es decir, fácilmente accesible inclusive a personal no encargado, se aconseja elegir estructuras cerradas para proteger los equipos y las conexiones realizadas.

Además, es indispensable instalar el armario de manera que se respete la distancia. Por lo tanto, es aconsejable instalarlo equidistante de cada toma usuario y las dimensiones deben ser tales que permitan alojar no sólo los paneles actuales y equipos activos, sino también eventuales expansiones de red que el usuario final pedirá en un futuro.

**5.- Cableado Horizontal**

El cable para la distribución de planta representa uno de los elementos más críticos de un cableado horizontal en relación con el impacto en los parámetros de las prestaciones del cableado realizado.

Estas afirmaciones valen no sólo en términos de calidad del producto utilizado, sino también desde el punto de vista de la precisión de la instalación ejecutada, ya que errores en el tendido del cable comprometen sensiblemente el rendimiento de la instalación.

Cabe recordar cómo las consecuencias de anomalías en la red derivadas de inconvenientes relativos al cableado comportan intervenciones caras por parte del instalador que debe ejecutar nuevamente el tendido con notable gasto de tiempo y parada de la red.

Para los sistemas de cableado estructurado de red de datos, el estándar utilizado para la distribución horizontal desde el armario de planta hasta la toma usuario es el cable retorcido de 4 pares equilibrados y trenzados disponibles en el mercado en las siguientes versiones:

- Cable de 4 pares no blindado de tipo UTP (unshielded twisted pairs).
- Cable par trenzado blindado STP (shielded twisted pair).
- Cable de fibra óptica 62.5/125um, dos fibras.

La dimensión del conducto permitido por los estándares va desde los 22 hasta los 26 AWG: la medida de 24 AWG es la más utilizada y corresponde a 0,5 mm de diámetro, con conductor de cobre sólido.

**El Dimensionamiento**

El dimensionamiento de la cantidad de cable necesaria en la instalación se debe realizar midiendo concretamente la ruta desde el armario de planta hasta todos los puestos de trabajo a cablear.

Este cálculo se debe efectuar para cada puesto de trabajo y para cada servicio suministrado en cada puesto (telefonía, datos, etc.). El cableado Horizontal no debe ser mayor a 90 m.

**Corrida Única**

La corrida única es la opción que generalmente se utiliza. Es una corrida de cable que no lleva puntos de interconexión y abarca desde el Armario de Telecomunicaciones hasta el Área de Trabajo.

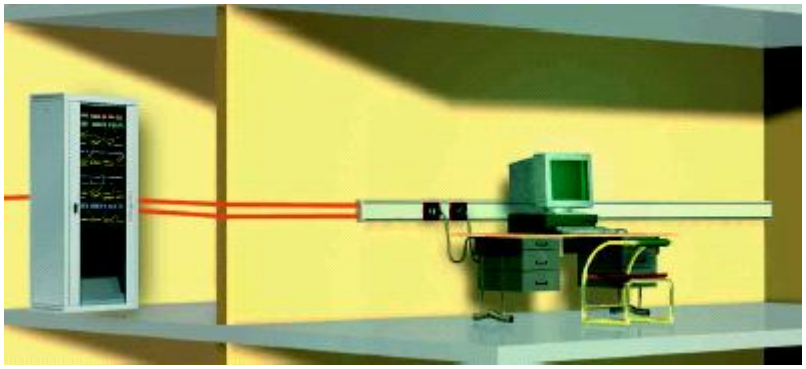


***Figura Nº 27 Corrida Única: Cuarto Telecomunicaciones / Área de Trabajo***

**Punto de consolidación**

El punto de consolidación es un punto de interconexión en el cableado horizontal y es el sistema preferido cuando se anticipa una cantidad limitada de cambios.

No es un empalme, se realiza a través de:

- Plug/Jack
- Sistema 110

Recomendaciones para el punto de consolidación:

- No utilizar panel de parcheo como punto de consolidación.
- Nunca se usará un Punto de Consolidación para equipo activo.
- Solo se permite un Punto de Consolidación entre cada corrida de cable.
- El punto de consolidación debe estar a más de 15 metros del Armario de Telecomunicaciones para reducir efectos de NEXT por múltiples conexiones.
- Cada Punto de Consolidación debe dar servicio a un máximo de 12 áreas de trabajo.
- Debe quedar instalado permanentemente, en un lugar accesible para cambios.
- La distancia de canal está limitada a 90m más 10m de cordones de parcheo. Siendo esta un total de 100m.

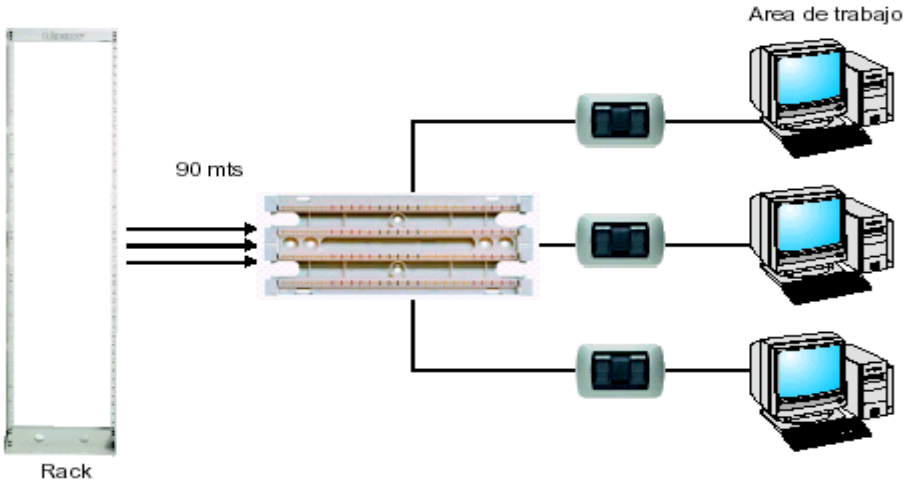



***Figura Nº 28 Punto de Consolidación***

**Salida multiusuario (MUTO)**

La salida multiusuario (MUTO) es un sistema que puede ofrecer cambios fáciles para remodelaciones en oficinas abiertas. Cables de conexión (cordones de parcheo) de estación son ruteados directamente del MUTO al área de trabajo. Es la solución preferida para aplicaciones donde se anticipan movimientos frecuentes.

Recomendaciones:

- Cada MUTO debe dar servicio a un máximo de 12 áreas de trabajo.
- Debe ser fácilmente accesible y no estar localizado en un piso o techo falso.
- Aún cuando la distancia del MUTO sea menor a 70m, la longitud máxima del cable de conexión (cordón de parcheo) de estación no deberá rebasar los 27m para 24 AWG ó 17m para 26 AWG.
- La distancia máxima nunca rebasará 100m.

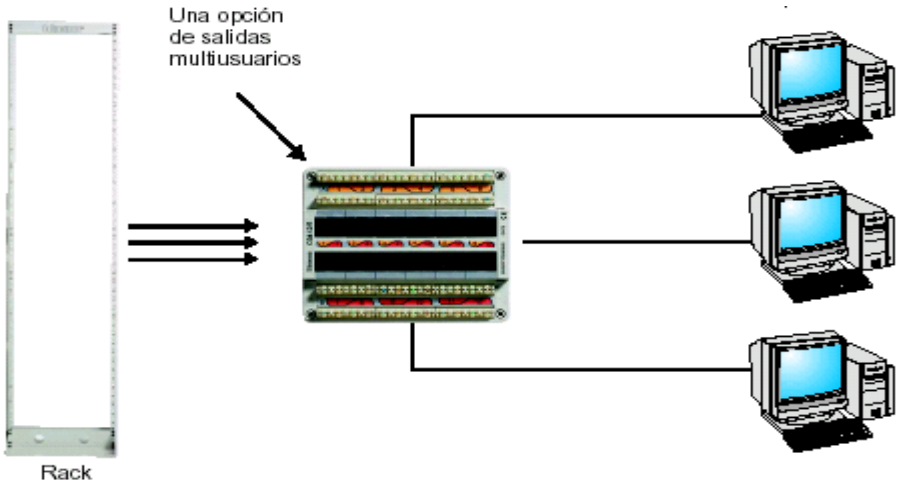



**Figura Nº 29 Salida Multiusuario**

### 6.- Área de trabajo

Comprende los elementos que se encuentran entre la toma del usuario y el equipo terminal.

Forman parte del área de trabajo la computadora, impresora, el cable de conexión y eventuales adaptadores.

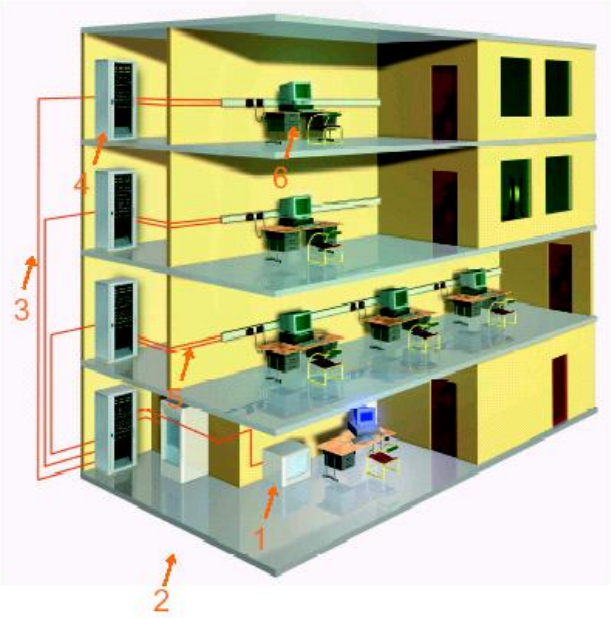



**Figura Nº 30 Modelo de un Cableado Estructurado**

## 4.2 NORMATIVIDAD INTERNACIONAL DEL CABLEADO ESTRUCTURADO

Cuando en 1985 en los Estados Unidos fue votada la desregulación, estaba claro que se precisaban normas que delineasen las características de un cableado estructurado y guiaran a los fabricantes, diseñadores e instaladores en la instalación de productos que respondieran en modo adecuado a las exigencias.

En 1991 EIA (Electronic Industries Association) y la consociada TIA (Telecommunications Industry Association) han puesto a punto un estándar denominado EIA/TIA-568 que representa la primera normativa más importante en materia de estándares de cableado.

A esta norma, que se refieren principalmente a los componentes de cableado, se une la 569A, relativamente a la instalación y la 606 que examina las infraestructuras.

La evolución tecnológica ha impuesto numerosas revisiones que han llevado a la versión actual denominada 568A. Contemporáneamente otros dos organismos ISO y CENELEC se han interesado en los sistemas de cableado, proponiendo el estándar ISO/IEC 11801 y el CENELEC 50173.

Ambas normas han retomado al menos una parte de lo afirmado por la EIA/TIA, introduciendo algunos particulares.

El estándar EIA/TIA 568 representa el documento de referencia para quienes desean acercarse al mundo del cableado estructurado.

## 4.3 ESTÁNDARES DE FACTO Y NORMADO

Un Estándar de Facto es creado cada vez que un comprador acepta y continúa comprando un determinado producto en grandes cantidades. Un ejemplo común de este caso es el diseño de las teclas del teclado de una computadora. Si una cantidad considerable de personas prefiere comprar un producto este producto es considerado un Estándar de Facto.

Los Estándares Normados existen de manera mucho más formal, típicamente se forma un comité. Este comité es constituido por conocidos miembros de la industria. Ellos desarrollan unas bases, desarrollan opiniones y

elaboran documentos, votan y eventualmente proceden a la publicación de los detalles del Estándar. Tales comités son formados en cada industria y en todos los niveles del gobierno.

En la industria de la computación, los fabricantes toman pasos activos para que sus productos sean adoptados como estándares de facto o normados.

Un estándar permite a un comprador obtener un producto dado desde una variedad de vendedores con mínimo riesgo de incompatibilidad.

## 4.4 ORGANIZACIONES ENCARGADAS DE ELABORAR LOS ESTÁNDARES

- INSTITUTO NACIONAL DE ESTANDAR AMERICANO (ANSI).
- TELECOMMUNICATIONS INDUSTRY ASSOCIATION / ASOCIACIÓN DE INDUSTRIAS DE TELECOMUNICACIONES (TIA).
- CANADIAN STANDARDS ASSOCIATIONS / ASOCIACIÓN DE ESTANDARES CANADIENSES (CSA).
- INTERNATIONAL ORGANIZATION FOR STANDARIZATION/INTERNATIONAL ELECTROTECHNICAL COMMISION (ISO/IEC).
- ELECTRONIC INDUSTRIES ALLIANCE / ASOCIACIÓN DE INDUSTRIA ELECTRÓNICA (EIA)

## 4.5 ESTÁNDARES DE CABLEADO

Los Grupos de Trabajo antes mencionados, bajo la jurisdicción de los subcomités TR-41.7 y TR-41.8 y aprobado por el comité técnico TR-41, han desarrollado una serie de estándares técnicos en Cableado de Edificios para productos y servicios de Telecomunicaciones.

Estos documentos cubren una necesidad reconocida en la industria de las telecomunicaciones y su relación con la estructurad de la industria.

Los más conocidos estándares de telecomunicaciones son:

ANSI/TIA/EIA 568-B Commercial Building Telecommunications Cabling Standard.

ANSI/TIA/EIA 569-B Commercial Building Standard for Telecommunications Pathways and Spaces.

ANSI/TIA/EIA 570 Residential and Light Commercial Telecommunications Wiring Standard.

ANSI/TIA/EIA 606 Administration Standard for the Telecommunications Infrastructure of Commercial Building.

ANSI/TIA/EIA 607 Grounding and Bounding Requirements for the Telecommunications in Commercial Buildings.

### 4.5.1 El Estándar ANSI/TIA/EIA 568B

El documento ANSI/TIA/EIA-568-B substituyó en 2001 el ANSI/TIA/EIA-568-A como el "Padrón de Cableado de Telecomunicaciones en Edificios Comerciales". Los apéndices 1 hasta 5 del documento 568 A y todos los TSBs

(Technical Systems Bulletins 62, 67, 72, 75 y 95) fueron incorporados al padrón 568-B.

B.1 - "Comercial Building Telecommunications Cabling Standard"

B.2 - "Balanced Twisted Pair Cabling Components"

B.3 - "Optical Fiber Cabling Components Standard"

Es decir: “Este estándar especifica un sistema de cableado de telecomunicaciones genérico para edificios comerciales que soportarán ambientes multiprotocolos o multifabricantes. Además provee orientación para el diseño de productos de telecomunicaciones comerciales”.

Este estándar se subdivide en tres partes fundamentales para un cableado estructurado:

ANSI/TIA/EIA 568B-1

Este padrón incorpora y modela de nuevo el contenido técnico de los siguientes documentos:

- TIA/ EIA TSB 67, Transmission Performance Specifications for Field Testing of Unshielded Twisted Pair Cabling Systems.
- TIA/ EIA TSB 72, Centralized Optical Fiber Cabling.
- TIA/ EIA TSB 75, Additional Horizontal Cabling Practices for Open Offices.
- TIA/ EIA TSB 95, Additional Transmission Performance Guidelines for 4-Pair 100 Ohms Category 5 Cabling.
- ANSI/ TIA/ EIA-568-A-1, Propagation Delay and Delay Skew Specifications for 100 Ohms 4 Pair Cable.

- ANSI/ TIA/ EIA-568A-2, Corrections and Additions to TIA/EIA-568-A.
- ANSI/ TIA/ EIA-568-A-3, Performance Specifications for Hybrid Cables.
- ANSI/ TIA/ EIA-568-A-4, Production Modular Cord NEXT Loss Test Method and Requirements for Unshielded Twisted Pair Cabling.
- ANSI/ TIA/ EIA--568-A-5, Transmission Performance Specifications for 4 Pair 100 Ohms Category 5e Cabling.
- TIA/ EIA/ IS-729, Technical Specifications for 100 Ohms Screened Twisted Pair Cabling.

Los elementos de la estructura de sistema de cableado de telecomunicaciones definidos de nuevo por la ANSI/EIA/TIA 568-B son:

- Servicio de entrada del Edificio.
- Cuarto de Equipos.
- Cableado Backbone.
- Cableado Horizontal.
- Área de Trabajo.

**Servicio de Entrada del Edificio**

Se corresponde con la definición del estándar TIA-569. Se define como el lugar en el que ingresan los servicios de telecomunicaciones al edificio y/o dónde llegan las canalizaciones de interconexión con otros edificios de la misma corporación (por ejemplo, si se trata de un “campus”).

Las “instalaciones de entrada” pueden contener dispositivos de interfaz con las redes publicas prestadoras de servicios de telecomunicaciones, y también equipos de telecomunicaciones. Estas interfaces pueden incluir borneras (por ejemplo telefónicas) y equipos activos (por ejemplo modem).

El “Punto de demarcación”, límite de responsabilidades entre los prestadores de servicio y las empresas que ocupan el edificio, se encuentra típicamente en esta sala. Estos “puntos de demarcación” pueden ser las borneras de terminación del cableado de planta externa, o equipos activos (por ejemplo módems HDSL). En éste último caso, estos equipos activos provistos por los prestadores de servicios también pueden ubicarse en las “Sala de Equipos”.

**Cuarto de Equipos**

La estructura general del cableado se basa en una distribución jerárquica del tipo “estrella”, con no más de 2 niveles de interconexión. El cableado hacia las “áreas de trabajo” parte de un punto central, generalmente la “Sala de Equipos”. Aquí se ubica el Distribuidor o Repartidor principal de cableado del edificio. Partiendo de éste distribuidor principal, para llegar hasta las áreas de trabajo, el cableado puede pasar por un Distribuidor o Repartidor secundario y por un Armario o Sala de Telecomunicaciones.

El estándar no admite más de dos niveles de interconexión, desde la sala de equipos hasta el Armario de Telecomunicaciones. Estos dos niveles de interconexión brindan suficiente flexibilidad a los cableados de backbone.

El “Distribuidor o repartidor principal de cableado” se encuentra típicamente en la “Sala de Equipos”. A este repartidor llegan los cables de los

equipos comunes al edificio (PBX, Servidores centrales, etc.) y son “cruzados” hacia los cables de distribución central (cables “montantes” o de “Backbone”).

El distribuidor o repartidor principal (a veces llamado MDF = “Main Distributoin Frame”) puede estar constituido por “regletas”, “patcheras” u otros elementos de interconexión. Generalmente está dividido en dos áreas, una a la que llegan los cables desde los equipos centrales (por ejemplo PBX) y otra a la que llegan los cables de distribución central (backbone).

**Cableado Backbone**

La función del “backbone” es proveer interconexión entre los armarios de telecomunicaciones y las salas de equipos y entre las salas de equipos y las instalaciones de entrada.

Los sistemas de distribución central de cableado incluyen los siguientes componentes:

- Cables montantes.
- Repartidores principales y secundarios.
- Terminaciones mecánicas.
- Cordones de interconexión o cables de cruzadas para realizar las conexiones entre distintos cables montantes.

El diseño de los sistemas de distribución central de cableado deben tener en cuenta las necesidades inmediatas y prever las posibles ampliaciones futuras, reservando lugar en el diseño de las canalizaciones, previendo cables con la cantidad adecuada de conductores, diseñando la cantidad de regletas o elementos de interconexión en los repartidores principales e intermedios, etc.

El esquema de la distribución central de cableado debe seguir la jerarquía en forma de estrella indicada en 5.2.2, de manera de no tener más de 2 puntos de interconexión desde los equipos hasta los puntos de interconexión horizontal (Armario de Telecomunicaciones).

El estándar admite los siguientes cables para el Backbone:

- Cables UTP de 100 ohm (par trenzado sin malla).
- Cables de Fibra óptica multimodo de 50/125 µm.
- Cables de Fibra óptica multimodo de 62.5/125 µm.
- Cables de Fibra óptica monomodo.
- Cable STP-A de 150 ohm (par trenzado con malla).

Los cables coaxiales, ya no están admitidos en el estándar. El cable STP-A de 150 ohm, si bien es admitido, no se recomienda para instalaciones nuevas.

La elección del tipo de cable y la cantidad de pares a utilizar depende de los servicios existentes y los futuros previstos. Para servicios telefónicos “clásicos”, se debe disponer de cables de cobre (UTP), a razón de un par por cada servicio telefónico (interno, fax, modem, etc.). Los servicios telefónicos comunes necesitan típicamente de un par para funcionar, mientras que servicios especiales pueden requerir de dos o más pares (por ejemplo, teléfonos con “ampliaciones de botoneras”, consolas de telefonista, etc.).

Asimismo, algunas PBX que disponen de teléfonos “híbridos” requieren de 2 pares por cada uno de éstos teléfonos. Es recomendable prever un crecimiento de por lo menos un 50% respecto a la cantidad de cables necesarias inicialmente.

A diferencia de los servicios telefónicos clásicos, los servicios de datos (o de telefonía IP) generalmente no requieren de pares de cobre desde la sala de equipos. Este tipo de servicios generalmente puede soportarse mediante el tendido de Fibras Ópticas, desde la sala de equipos (o centro de cómputos) hasta los armarios de telecomunicaciones. Por esta razón, los tendidos de backbone generalmente se componente de cables UTP y de cables de Fibras ópticas, en número apropiada para las necesidades presentes y previsiones futuras.

Las distancias máximas para los cables montantes dependen de las aplicaciones (telefonía, datos, video, etc.) que deban transmitirse por ellas.

Como reglas generales, el estándar establece las distancias máximas presentadas a continuación:

| Tipo de Cable | Armario de Telecomunicaciones hasta Distribuidor Principal | Armario de Telecomunicaciones hasta Distribuidor Secundario | Distribuidor Secundario hasta Distribuidor Principal |
|---|---|---|---|
| UTP | 800 m | 300 m | 500 m |
| Fibras ópticas Multimodo | 2.000 m | 300 m | 1.700 m |
| Fibras ópticas Monomodo | 3.000 m | 300 m | 2.700 m |

***Figura Nº 31 Estándares de Distancias Máximas de Cableado***

Es de hacer notar que no todas las aplicaciones podrán funcionar adecuadamente con estas distancias máximas. Por ejemplo, si se tener transmisión de datos sobre UTP en el backbone, la distancia máxima para su correcto funcionamiento será de 90 m (y no 800 m como indica el máximo del estándar).

Cableado Horizontal

Los cables montantes (backbone) terminan en los distribuidores o repartidores horizontales, ubicados en la Sala o Armario de Telecomunicaciones. Estos repartidores horizontales deben disponer de los elementos de interconexión adecuados para la terminación de los cables montantes (ya sean de cobre o fibra óptica).

Asimismo, a los repartidores horizontales llegan los cables provenientes de las “áreas de trabajo” (cableado horizontal, de allí su nombre de “repartidores horizontales”), el que también debe ser terminado en elementos de interconexión adecuado.

La función principal de los repartidores horizontales es la de interconectar los cables horizontales (provenientes de las áreas de trabajo) con los cables montantes (provenientes de la sala de equipos).

Eventualmente, en la Sala o Armario de Telecomunicaciones, puede haber equipos de telecomunicaciones, los que son incorporados al repartidor horizontal para su interconexión hacia la sala de equipos (a través del backbone) y/o hacia las áreas de trabajo (a través del cableado horizontal). Típicamente los repartidores horizontales, ubicados en los armarios de telecomunicaciones, consisten en “paneles de interconexión”, en los que terminan los cableados horizontales y los cableados de backbone. Estos paneles de interconexión permiten, mediante el uso de “cables de interconexión”, conectar cualquier cable horizontal con cualquier cable de backbone o equipo activo.

Los paneles de interconexión pueden ser “patcheras” con conectores del tipo RJ - 45 o “regletas” de diversos formatos. Sin embargo, estos paneles

deben cumplir con las características mecánicas y eléctricas que se especifican en los estándares de acuerdo a la “categoría” (5e, 6, etc.) del sistema. De la misma manera, los cables de interconexión (generalmente llamados “patch cords” o cordones de patcheo) también deben cumplir con las características mecánicas y eléctricas de acuerdo a su “categoría”.

En el caso de disponer de equipos activos en el armario de telecomunicaciones (típicamente hubs, switches, etc.), se admite conectar directamente los paneles del cableado horizontal a los equipos activos, mediante cables de interconexión adecuados (por ejemplo cordones de patcheo).

La distribución horizontal es la parte del cableado de telecomunicaciones que conecta las áreas de trabajo con los distribuidores o repartidores horizontales, ubicados en el Armario o Sala de Telecomunicaciones.

La distribución horizontal incluye:

- Cables de distribución horizontal.
- Conectores de telecomunicaciones en las áreas de trabajo (dónde son terminados los cables de distribución horizontal).
- Terminaciones mecánicas de los cables horizontales.
- Cordones de interconexión (“patch cords”) en el Armario o Sala de Telecomunicaciones.
- Puede incluir también “Puntos de Consolidación”

El cableado de distribución horizontal debe seguir una topología del tipo “estrella”, con el centro en el armario o sala de telecomunicaciones, y los extremos en cada una de las áreas de trabajo. Los conectores de

telecomunicaciones en las áreas de trabajo deben ser conectados mediante un cable directamente al panel de interconexión ubicado en el armario de telecomunicaciones. No se admiten empalmes ni uniones, salvo en caso de existir un “punto de consolidación”

La distancia máxima para el cable de distribución horizontal es de 90m, medida en el recorrido del cable, desde el conector de telecomunicaciones en el área de trabajo hasta el panel de interconexión en el armario de telecomunicaciones.

Los cordones de interconexión (“patch cords”) utilizados en las áreas de trabajo y en el armario de telecomunicaciones no deben ser más largos que 10 m en conjunto (completando una distancia de 100 m de “punta a punta”. Se recomienda que los cordones de interconexión en cada extremo no superen los 5 m.

Los cables reconocidos para la distribución horizontal son:

- UTP o ScTP de 100  y cuatro pares.
- Fibra óptica multimodo de 50/125 µm.
- Fibra óptica multimodo de 62.5/125 µm.
- Cable STP-A de 150, este cable es aún reconocido pero no recomendado para nuevas instalaciones.

Cada área de trabajo debe estar equipada con un mínimo de 2 conectores de telecomunicaciones. Uno de ellos típicamente es asociado con servicios de “voz” y el otro con servicios de “datos”, aunque esta distinción puede de hecho no existir.

Uno de los conectores del área de trabajo debe estar conectado a un cable UTP de 100 y cuatro pares, de categoría 3 o superior, aunque para instalaciones nuevas se recomienda categoría 5E o superior.

El segundo de los conectores del área de trabajo debe estar conectado a algunos de los siguientes tipos de cables:

- UTP de 100 y cuatro pares, de categoría 5E o superior.
- 2 cables de Fibra óptica multimodo de 50/125 µm.
- 2 cables de Fibra óptica multimodo de 62.5/125 µm.

En el diseño de cada instalación se debe decidir la tecnología más conveniente para el cableado horizontal. Es muy común en áreas de oficinas utilizar únicamente cableado de cobre (UTP) para los 2 o más conectores en las áreas de trabajo. En este caso es altamente recomendable que todos ellos sean de categoría 5E o superior, a pesar de que la norma admite que uno de ellos sea de categoría inferior.

**Cableado Horizontal en "oficinas abiertas"**

Como se describió en los capítulos anteriores, el cableado horizontal consiste en tramos "rígidos" de cable, que comienzan en los armarios de telecomunicaciones y terminan en las áreas de trabajo. Los puntos "flexibles" existen únicamente dentro de los armarios de telecomunicaciones (dónde puede interconectarse cualquier área de trabajo a cualquier equipo o cable de backbone) y en las propias áreas de trabajo (dónde mediante patch cords pueden conectarse los PCs, teléfonos, impresoras, etc.)

Sin embargo, en varios edificios comerciales, las oficinas tienen cierta movilidad.

Es común encontrar oficinas del tipo “boxes”, dónde las divisiones son realizadas con componentes livianos (madera, yeso, tabiques, etc.). La disposición de estas oficinas puede variar con el tiempo, de acuerdo a los nuevos requerimientos locativos de las empresas. Recordando que los sistemas de cableado estructurado están pensados para una vida útil de 15 a 25 años, resulta claro que el cableado horizontal requiere de cierta “movilidad” que hasta ahora no ha sido contemplada.

Es por esto que se ha incluido en la recomendación la posibilidad de incluir dos tipos de sistemas que permiten cierta flexibilidad en el cableado horizontal:

**Dispositivos de múltiples conectores de telecomunicaciones (“Multi-User Telecommunications Outlet Assembly”)**

Los “Dispositivos de múltiples conectores de telecomunicaciones” son puntos de terminación del cableado horizontal consistentes en varios conectores en una misma “caja”, típicamente ubicada en puntos cercanos a varias áreas de trabajo.

Desde estos puntos, pueden tenderse cordones modulares (del tipo “patch cords”) de hasta 20 m, los que deben ser conectados directamente a los equipos de las áreas de trabajo. Los cables horizontales que parten del repartidor horizontal son terminados en forma fija (rígida) a los conectores ubicados en los “Dispositivos de múltiples conectores de telecomunicaciones”.

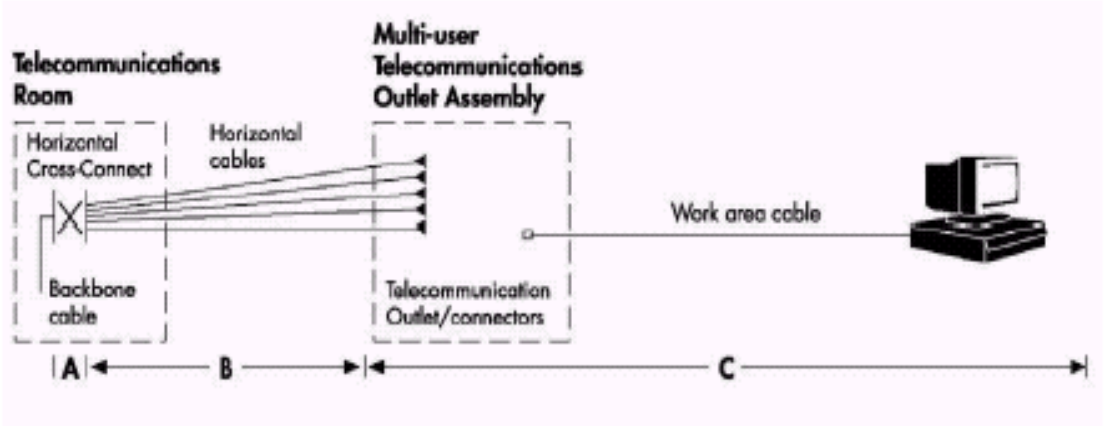



***Figura Nº 32  Dispositivo Múltiple de Conexiones***

Estas “cajas” (“Dispositivos de múltiples conectores de telecomunicaciones”) deben ser ubicadas en lugares accesibles. No se admite que estén sobre el cielorraso. Cada uno de los cordones de interconexión que parten de estos puntos, hasta las áreas de trabajo, deben estar debidamente etiquetados en ambas puntas, con identificadores únicos.

Un mismo “Dispositivo de múltiples conectores de telecomunicaciones” puede tener hasta 12 conectores.

Las distancias máximas desde los “Dispositivo de múltiples conectores de telecomunicaciones” hasta las áreas de trabajo pueden variar, de acuerdo a las distancias de los cables horizontales que llegan a estos dispositivos, de manera que las distancia total (“punta a punta”) no supere los 100 m. La siguiente tabla indica las distancias máximas admisibles, en función de los tramos marcados como “A”, “B” y “C” en la figura anterior:

| Tramo "A" (m) | Tramo "B" (m) | Tramo "C" (m) | Distancia total (m) |
|---|---|---|---|
| 5 | 90 | 5 | 100 |
| 5 | 85 | 9 | 99 |
| 5 | 80 | 13 | 98 |
| 5 | 75 | 17 | 97 |
| 5 | 70 | 22 | 97 |

***Figura Nº 33 Distancias Máximas por tramos***

En la caja que contiene a los múltiples conectores de telecomunicaciones debe indicarse claramente cual es la distancia máxima de los cables modulares de interconexión.

**Puntos de Consolidación**

Los "puntos de Consolidación" son lugares de interconexión entre cableado horizontal proveniente del repartidor horizontal y cableado horizontal que termina en las áreas de trabajo o en los "Dispositivo de múltiples conectores de telecomunicaciones".

Dado que el cableado horizontal es "rígido", la idea es tener un punto intermedio que permita, en caso de reubicaciones de oficinas (y por lo tanto de áreas de trabajo), re-cablear únicamente parte del cableado horizontal (el que va desde el punto de consolidación hasta las nuevas áreas de trabajo).

El punto de consolidación no es un punto de "interconexión flexible", sin un punto de "interconexión rígido". Las reconexiones ocurren únicamente cuando se mueven las áreas de trabajo y es necesario tender nuevos cables. En estos casos, en lugar de tender nuevos cables hasta los armarios de telecomunicaciones, pueden tenderse nuevos cables hasta los "puntos de

consolidación", y mantener los cables desde estos puntos hasta los armarios de telecomunicaciones.

Como puede verse, los puntos de consolidación son útiles para prever futuros cambios en los lugares de las áreas de trabajo, pero no tan frecuentes como para que requieran de "Dispositivos de múltiples conectores de telecomunicaciones".

Cuando existen puntos de consolidación, la distancia total de cable, desde el área de trabajo, hasta el armario de telecomunicaciones (incluyendo el pasaje por el punto de consolidación) no debe exceder los 90 m.

Se recomienda que los puntos de consolidación, de ser necesarios, estén a más de 15 m del armario de telecomunicaciones, para evitar efectos adicionales que se pueden producir en tramos cortos de cables, producidos por "rebotes" en los puntos de interconexión.

No se admite más de un punto de consolidación por cada cable horizontal. Un mismo punto de consolidación puede servir hasta 12 áreas de trabajo.

Área de Trabajo

Las áreas de trabajo incluyen los conectores de telecomunicaciones y los cordones de interconexión ("Patch-cords") hasta el equipamiento (por ejemplo, PC, teléfono, impresora, etc.). El tipo de equipamiento que se instale en las áreas de trabajo no es parte de recomendación.

Se recomienda que la distancia del cordón de interconexión no supere los 5m. Los cables UTP son terminados en los conectores de telecomunicaciones en "jacks" modulares de 8 contactos, en los que se

admiten dos tipos de conexiones, llamados T568A y T568B. Esta denominación no debe confundirse con el nombre de la norma ANSI/TIA/EIA 568-A o ANSI/TIA/EIA 568-B, ya que representan cosas bien diferentes. La norma actualmente vigente es la ANSI/TIA/EIA 568-B, en la que se admiten dos formas de conectar los cables en los conectores modulares.

Estas dos formas de conexión son las que se denominan T568A y T568B.

La siguiente figura indica la disposición de cada uno de los hilos en un cable UTP, para ambos tipos de conexiones:

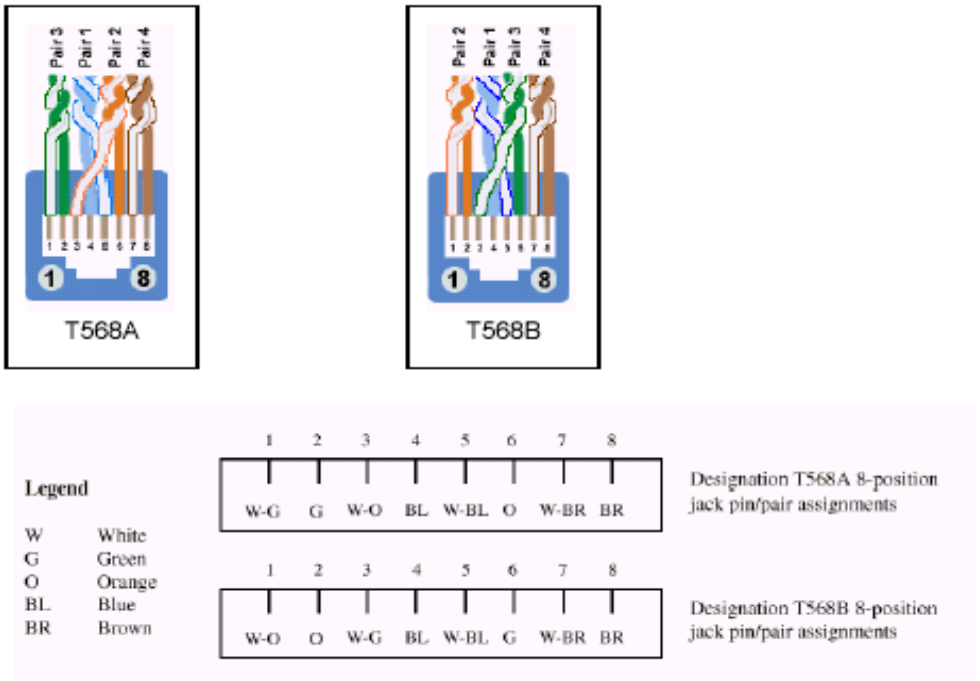



Figura Nº 34 Cableado UTP (Modos de Conexión)

Los cables de fibra óptica son terminados en el área de trabajo en conectores dobles, es decir, que permiten la terminación de dos hilos de fibra.

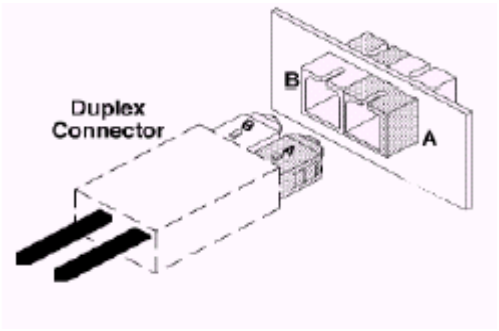



**Figura Nº 35 Adaptadores para Conexión de Fibra Óptica**

Se recomienda utilizar el conector 568SC, pero se admiten otros tipos de conectores de dimensiones adecuadas. La figura muestra un conector del tipo 568SC y un cordón de interconexión de fibra óptica con su correspondiente terminación 568SC.

ANSI/TIA/EIA 568B-2

Este estándar especifica las características de los componentes del cableado, incluyendo parámetros mecánicos, eléctricos y de transmisión.

El estándar reconoce las siguientes categorías de cables:

- **Categoría 3**: Aplica a cables UTP de 100 y sus componentes de conexión, para aplicaciones de hasta 16 MHz de ancho de banda.
- **Categoría 4**: Aplicaba a cables UTP de 100 y sus componentes de conexión, para aplicaciones de hasta 20 MHz de ancho de banda. Sin embargo, esta categoría ya no es reconocida en el estándar.

- **Categoría 5**: Aplicaba a cables UTP de 100 y sus componentes de conexión, para aplicaciones de hasta 100 MHz de ancho de banda. Sin embargo, esta categoría ha sido sustituida por la 5e, y ya no es reconocida en el estándar.
- **Categoría 5e**: Aplica a cables UTP de 100 y sus componentes de conexión, para aplicaciones de hasta 100 MHz de ancho de banda. Se especifica para esta categoría parámetros de transmisión más exigentes que los que aplicaban a la categoría 5.
- **Categoría 6**: Aplica a cables UTP de 100 y sus componentes de conexión, para aplicaciones de hasta 200 MHz de ancho de banda. Se especifica para esta categoría parámetros de transmisión hasta los 250 MHz

Es de hacer notar que las categorías indican los parámetros de transmisión de los cables y los componentes de interconexión en función del "ancho de banda" medido en MHz, y no en bits por segundo.

Los cables reconocidos para el cableado horizontal deben tener 4 pares trenzados balanceados, sin malla (UTP = Unshielded Twisted Pair). Los conductores de cada par deben tener un diámetro de 22 AWG a 24 AWG.

**Características mecánicas de los cables para cableado horizontal:**

- El diámetro de cada cable no puede superar los 1.22 mm.
- Los cables deben ser de 4 pares únicamente. No se admite para el cableado horizontal cables de más o menos pares.

(Notar que si se admiten cables “multipares” para los backbones).

- Los colores de los cables deben ser los siguientes:

  Par 1: Azul-Blanco, Azul **(W-BL)(BL)**

  Par 2: Naranja-Blanco, Naranja **(W-O)(O)**

  Par 3: Verde-Blanco, Verde **(W-G)(G)**

  Par4: Marrón-Blanco, Marrón **(W-BR)(BR)**

- El diámetro completo del cable debe ser menor a 6.35mm.
- Debe admitir una tensión de 400 N.
- Deben permitir un radio de curvatura de 25.4 mm (1”) sin que los forros de los cables sufran ningún deterioro.

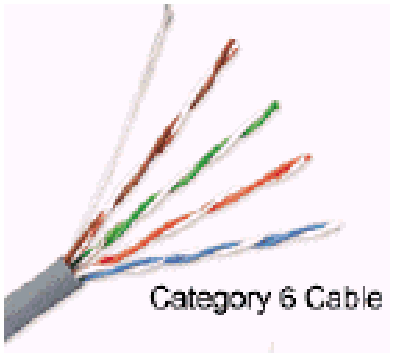



Figura Nº 36 Cableado UTP Categoría 6

**Características eléctricas de los cables para cableado horizontal:**

- La resistencia “en continua” de cada conductor no puede exceder los 9.38 por cada 100m a 20ºC.
- La diferencia de resistencias entre dos conductores del mismo par no puede superar en ningún caso un 5%.

- La capacitancia mutua de cualquier par de cables, medida a 1 kHz no puede exceder los 6.6nF en 100m de cable para Categoría 3 y 5.6nF en 100 m de cable para Categoría 5e.
- La capacitancia desbalanceada, entre cualquier cable y tierra, medida a 1kHz, no puede exceder los 330pF en 100m de cable.
- La impedancia característica del cable debe ser de 100 +/- 15% en el rango de las frecuencias de la categoría del cable.

**Características de transmisión de los cables para cableado horizontal**

El estándar establece varios requerimientos acerca de diversos parámetros relacionados con la transmisión. Más allá de presentar las tablas correspondientes (que pueden verse en el propio estándar), se realizará una presentación del significado de cada uno de éstos parámetros.

**Atenuación**

La atenuación en un canal de transmisión es la diferencia de potencias entre la señal inyectada a la entrada y la señal obtenida a la salida del canal. Los cables UTP son de hecho canales de transmisión, y por lo tanto, la potencia de la señal al final del cable (potencia recibida) será menor a la potencia transmitida originalmente.


Figura Nº 37 Atenuación

Esta diferencias de potencias, generalmente se mide en “decibeles” (dB), y depende de la frecuencia de la señal. Cuanto mayor es la frecuencia de la señal, más se atenúa al recorrer el medio de transmisión.

La figura siguiente muestra una gráfica típica de la atenuación de la señal en función de la frecuencia, para un cable de 100 m de longitud

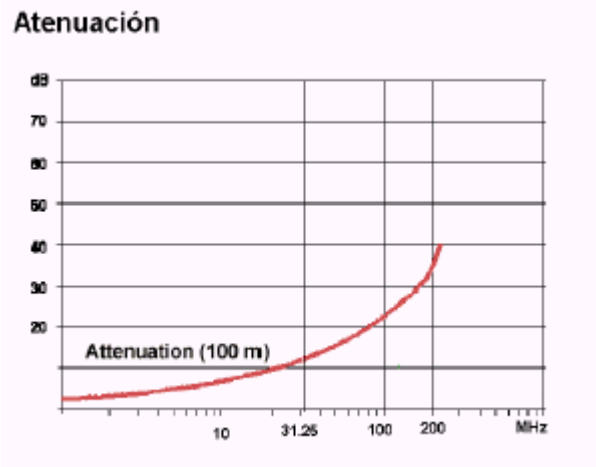



Figura Nº 38  Modo Gráfico de la atenuación (db/Mhz)

La diferencia de potencias entre la salida y la entrada se conoce también como “Pérdida de inserción” (“Insertion Loss”). Un valor bajo (en dB) indica poca pérdida de potencia, y por lo tanto, mayor nivel de señal de salida.

**Pérdida por Retorno**

Los cables UTP tienen una impedancia característica de 100. Sin embargo, ésta impedancia depende de la geometría del cable y de los cambios de medio.

A frecuencias altas, los cables se comportan como líneas de transmisión, y por lo tanto, pueden aplicarse los mismos conceptos. Las ondas

incidentes en una línea de transmisión pueden verse reflejadas debido a diferencias de impedancias (cambios en el factor þ, como puede verse en la figura).

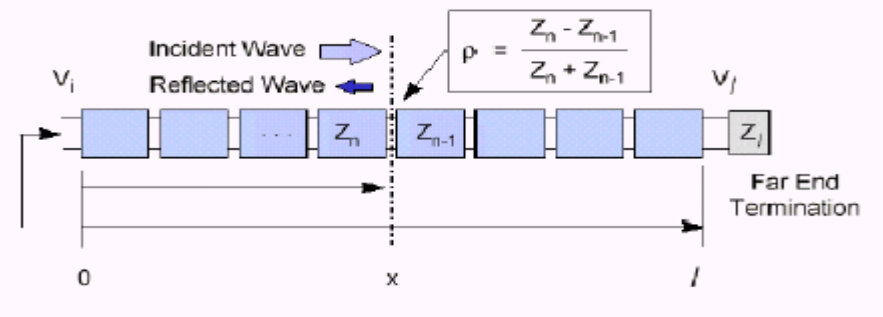



Figura Nº 39 Pérdida por Retorno

En una línea de transmisión, la señal es sensible a cambios en la geometría en distancias del orden de la décima parte de la longitud de onda de la señal. Para señales de 1 MHz, la longitud de onda es de unos 200m, y por lo tanto afectan a la impedancia cambios geométricos de unos 20m. Sin embargo, a 200 MHz, la longitud de onda es del orden de 1m, y por lo tanto, cambios geométricos en el tendido de un cable del orden de los 10cm pueden producir cambios de impedancia y por lo tanto señales reflejadas apreciables.

Los cambios de impedancia más acentuados se producen en los “cambios de medio”, los que se dan en los puntos de interconexión de los cables (es decir, en los conectores de telecomunicaciones en las áreas de trabajo, en los puntos de consolidación, en los paneles de interconexión de las salas de telecomunicaciones, etc.)

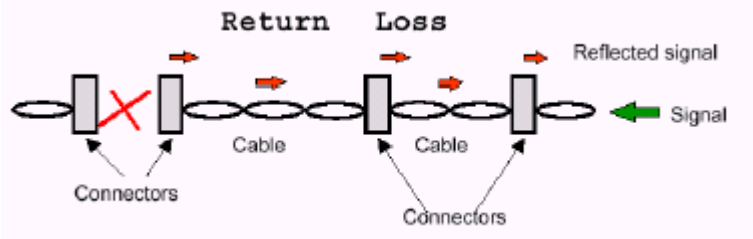



Figura Nº 40 Modo Perdida por Retorno, mediante conectores

Las pérdidas por retorno tienen tres efectos en los sistemas de cableado estructurado:

- El primero es aumentar la pérdida de inserción, lo que se ve reflejado como una menor potencia de señal en la salida del cable (sumando por lo tanto a la atenuación total de la señal).
- El segundo, es generar una señal reflejada, que viaja “hacia atrás”. En casos de utilizar el mismo par para transmisiones “full duplex”, esta señal reflejada se sumará como “ruido” a la señal de información realmente transmitida.
- El tercer efecto tiene que ver con las señales “re-reflejadas”, que vuelven a viajar “hacia delante”, pero que llegan a destino más tarde que la señal principal. Este fenómeno se conoce como “Desviación de la pérdida de inserción” (Insertion Loss Deviation), y se traduce en un ruido que se suma a la señal principal.

Este fenómeno es especialmente apreciable a frecuencias altas, y en tramos cortos de cable. La siguiente figura muestra la desviación por pérdida de inserción en función de la frecuencia para cada uno de los 4 pares de un cable UTP.

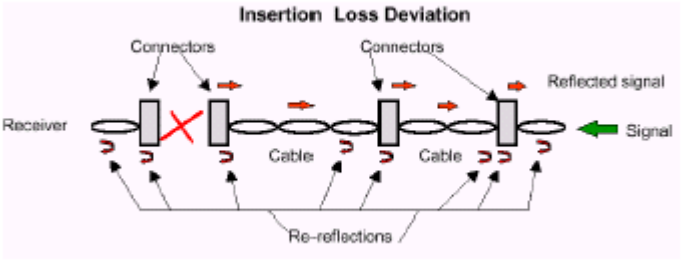



Figura Nº 41 Intersección de Desviación de Perdidas

**Diafonía (“Cross-talk”)**

La diafonía (o “Crosstalk”) se debe a la interferencia electromagnética de cada par de transmisión sobre los pares cercanos. Dado que el cableado horizontal consiste en cables de 4 pares, la mayor fuente de “ruido” de estos pares proviene de los pares adyacentes.

El crosstalk depende de la frecuencia de la señal, de la geometría de los cables, etc. Se mide como la potencia de la señal de interferencia respecto a la potencia de la señal transmitida.

Cuando se introduce una señal en un extremo de un par, esta señal produce interferencia sobre los pares cercanos. Esta interferencia se propaga por los cables cercanos en ambos sentidos, llegando por lo tanto a ambos extremos del cable “interferido”. La potencia de la señal de interferencia (“crosstalk”) recibida en el mismo extremo del cable que en el que se introdujo la señal original se denomina “diafonía de extremo cercano”. Típicamente se conoce por sus siglas en inglés: NEXT (“Near-end Crosstalk”). La potencia de la señal de interferencia (“crosstalk”) recibida en el extremo opuesto del cable respecto al que se introdujo la señal original se denomina “diafonía de extremo lejano”. Típicamente se conoce por sus siglas en inglés: FEXT (“Far-end Crosstalk”).

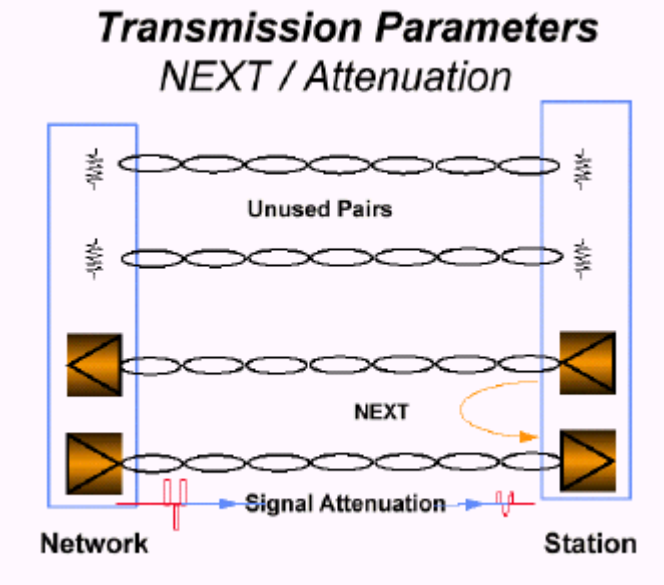



Figura Nº 42 Atenuación NEXT (Diafonía Extremo Cercano)

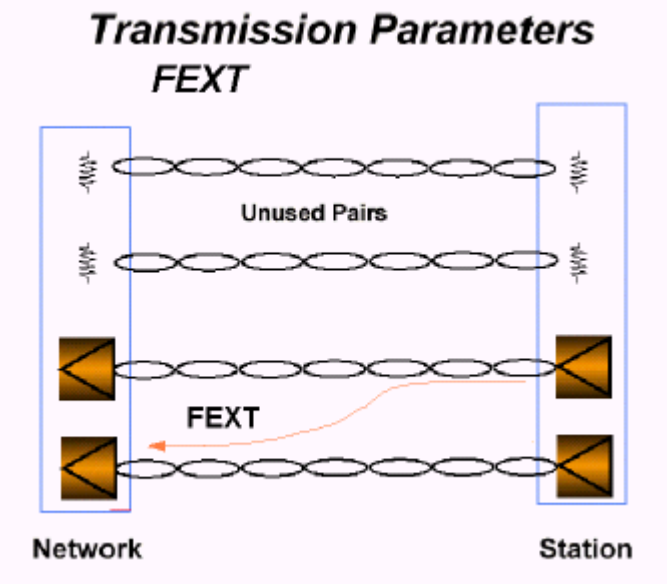



Figura Nº 43 Atenuación FEXT (Diafonía Extremo Lejano)

Hay que recordar que los cables admitidos para el cableado horizontal son de 4 pares, los que podrían usarse en forma simultánea y en modo bidireccional (como por ejemplo en aplicaciones Gigabit Ethernet). Esto

significa que los 4 pares estarán transmitiendo señales en ambos sentidos a la vez. Es por esto que hay que tener en cuenta la suma de interferencias (en ambos sentidos) sobre un determinado par.

Es por esta razón que se ha desarrollado el concepto de “suma de potencias de diafonía”, conocido en inglés como “Power Sum Cross-talk”, y más específicamente como “Power Sum NEXT” (PSNEXT) y “Power Sum FEXT” (PSFEXT), para las interferencias de extremos cercanos y extremos lejanos respectivamente.

Hasta la categoría 5, el estándar especificaba simplemente los valores límites del FEXT y del NEXT, ya que ésta categoría no estaba pensada para aplicaciones que utilizaran todos los pares en forma bidireccional. Sin embargo, a partir de la categoría 5e, el estándar especifica los valores límites de PowerSum FEXT y PowerSum NEXT, lo que torna más exigentes a los valores de FEXT y NEXT individuales (es decir, para que la suma de las potencias estén dentro de los parámetros exigidos, se debe ser más exigente con cada potencia de interferencia en forma individual)

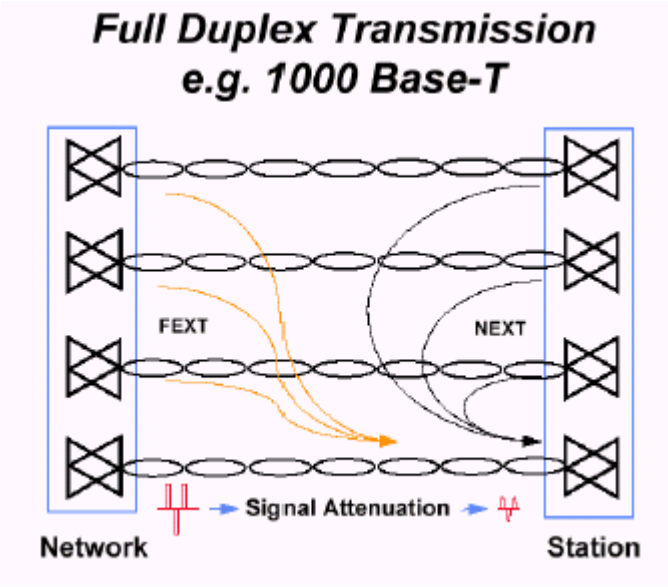



Figura Nº 44 Atenuación NEXT – FEXT en UTP Full Duplex

**ACR (Atenuation Crosstalk Ratio)**

La diafonía o crosstalk es la principal fuente de “ruido” o interferencia en un cable UTP. Por lo tanto, una buena medida de la relación señal a ruido en el receptor puede verse como la relación (señal atenuada) / (Power Sum Crosstalk). Por lo tanto, la relación entre la atenuación y el Powersum crosstalk brinda un umbral mínimo para la relación señal – ruido en la recepción, en un cable UTP.

El parámetro ACR (Attenuation to Crosstalk Ratio) se define como la diferencia (medida en dB) de la atenuación y la diafonía, y es una medida de la relación señal a ruido en el extremo receptor del cable. Cuando el ACR llega a 0, la potencia del ruido de interferencia iguala a la potencia de la señal recibida, por lo que se torna prácticamente imposible poder reconstruir la señal. Dado que el ACR disminuye al aumentar la frecuencia, el punto de ACR = 0 marca en cierta forma el ancho de banda utilizable del cable.

ACR es uno de los parámetros más importantes en los cables UTP, ya que de él depende el ancho de banda utilizable.

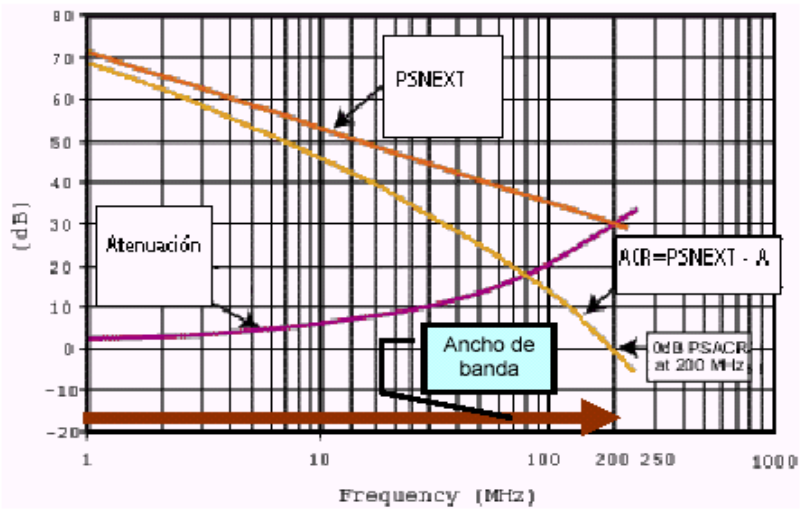


Figura Nº 45 ACR

**Retardo de Propagación**

El retardo de propagación es el tiempo que insume una señal en viajar desde un extremo al otro de un enlace. Se mide en ns (nano segundos), y depende levemente de la frecuencia. El estándar especifica los retardos aceptables en función de la frecuencia para cada categoría

**Diferencias de Retardo de Propagación (Delay Skew)**

Para aprovechar el máximo ancho de banda en un cable UTP de 4 pares, los códigos de línea dividen la señal a transmitir entre los 4 pares. El receptor debe reconstruir la señal tomando lecturas de los 4 pares en forma simultánea. Por esta razón, es importante que las señales lleguen al extremo lejano “al mismo tiempo”, o por lo menos con diferencias de tiempo mínimas.

La “diferencia de retardos” o “Delay Skew” mide la diferencia de retardos entre el par “más rápido” y el par “más lento”. El estándar establece los límites máximos para esta diferencia.

ANSI/TIA/EIA 568B-3

Este estándar especifica las características de los componentes y los parámetros de transmisión para un sistema de cableado de fibra óptica (cables, conectores, etc.), para fibras multimodo de 50/125 µm y 62.5/125 µm y fibras monomodo.

## Fibra Óptica

Muchas de las aplicaciones actuales de telecomunicaciones utilizan las fibras ópticas como medio de transmisión, ya sea en distribución entre edificios, como dentro de edificios, en backbone, o incluso llegando hasta las áreas de trabajo.

Las fibras ópticas son inmunes a interferencias electromagnéticas y a radio frecuencia, son livianas y disponen de un enorme ancho de banda. Esto, sumado al continuo descenso en su precio final, las hacen ideales para aplicaciones de voz, video y datos de alta velocidad.

## Evolución de la transmisión óptica

La teoría de utilizar la luz como medio de transmisión de información es muy antigua. En 1880, Alexander Graham Bell demostró que la luz podía transportar señales de voz por el aire, sin necesidad de utilizar cables. El “Fotofono” de Bell reproducía voces detectando las variaciones de luz solar que llegaban a un receptor. Su teoría era perfectamente correcta, pero no era práctica en esa época.

Durante 1930, se realizaron varias patentes que utilizaban “tubos” como guías de onda para la luz. Sin embargo, estos tubos eran grandes e imprácticos para aplicaciones comerciales.

El interés en las tecnologías de fibras ópticas comenzó a crecer significativamente por 1950, cuando se patentó un método que utilizaba un vidrio en forma cilíndrica, de dos capas como guía de onda para la luz.

El principio detrás de la guía de onda de dos capas es confinar la señal de luz dentro de la capa interior (núcleo), utilizando una capa exterior (cladding) que reflejara la luz haciendo que ésta permanezca siempre dentro del núcleo. Este principio se basa en la “Ley de Snell”, que relaciona los ángulos de refracción de la luz en un cambio de medio con los índices de refracción de cada medio:

$$\mathbf{n_1 Sen\theta_1 = n_2 Sen\theta_2}$$

$n_1$ y $n_2$ son los índices de refracción de cada medio. El $\theta_1$ es el ángulo de incidencia del haz de luz, proveniente del medio $n_1$ y $\theta_2$ es el ángulo con el que sale el haz de luz en el medio $n_2$.

Seleccionando adecuadamente los índices de refracción ($n_1 > n_2$), se puede obtener un ángulo crítico $\theta_c$ a partir del cual toda la luz previniente del medio $n_1$ es reflejada nuevamente hacia el medio $n_1$. (En este punto $\theta_2$= 90°)

$$\mathbf{\theta_c = arcsen\ (n_2 / n_1)}$$

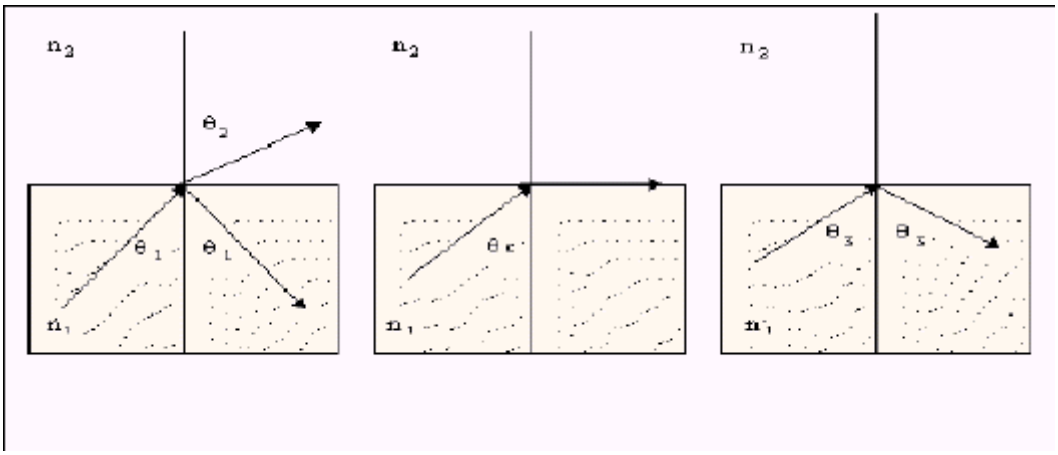


***Figura Nº 46  Trasmisiones Ópticas***

Es decir, si el ángulo de incidencia del haz de luz proveniente de $n_1$ es mayor a $\theta_c$ toda la luz es reflejada, y por lo tanto, se mantiene “confinada” dentro del medio $n_1$.

Este principio de funcionamiento es el fundamento de la transmisión por fibra óptica que se utiliza actualmente.

Sin embargo, era necesario disponer de una fuente de luz capaz de atravesar distancias grandes de éstas guías ópticas.

En los comienzos de 1960, se utilizó por primera vez un “Laser” como fuente de luz para las primeras fibras ópticas, con resultados asombrosos. Sin embargo, el alto costo de los láser ópticos de aquella época impedían el uso comercial de ésta tecnología.

A finales de 1960 se descubrió que las altas pérdidas de luz in las fibras ópticas eran debido mayoritariamente a las impurezas del vidrio, y no a sus propiedades intrínsecas.

A principios de 1970, los ingenieros de la “Corning Glass Works” refinaron el proceso de construcción de las fibras ópticas, consiguiendo pérdidas de luz mucho menores, y permitiendo el uso de fuentes de luz de menor costo, como los LEDs.

En 1980, las tecnologías de fibras ópticas comenzaron a encontrar su lugar como el “backbone” de las redes telefónicas de larga distancia en Estados Unidos.

Actualmente, con los avances de la tecnología digital y de fabricación de fibras y emisores de luz, las fibras ópticas se han convertido en parte integral de las redes de telecomunicaciones.

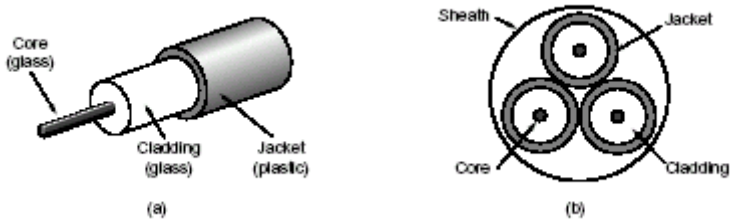



***Figura Nº 47 Figura: (a) Vista de lado de una fibra individual. (b) Vista de extremo de una envoltura con tres fibras***

**Sistemas de Fibra Óptica**

Un sistema de transmisión de fibra óptica tiene tres componentes básicos:

- Una fuente de luz o emisor óptico.
- Un receptor óptico.
- El medio óptico (fibra óptica)

**Emisores ópticos**

Los emisores ópticos reciben una señal eléctrica modulada y la convierten en una señal óptica modulada. El emisor óptico típicamente envía “pulsos ópticos”, encendiendo o apagando la fuente de luz, o cambiando la intensidad.

Existen dos tipos de emisores ópticos:

- **LED** (Light Emitting Diode). Es el componente de emisión óptica más barato, y se utiliza generalmente para cables relativamente cortos.

- **LASER** (Light Amplification by Stimulated Emission of Radiation). Son más caros que los LED, y son utilizados generalmente para cables de largas distancias.

Los emisores ópticos son categorizados según las siguientes características básicas:

**Longitud de onda central.** Las fibras ópticas no transmiten todas las frecuencias de luz con la misma eficiencia. La atenuación es generalmente mucho mayor para la luz visible que para la luz en la banda infrarroja.

Dentro de la banda infrarroja, hay ciertas longitudes de onda en las que las fibras ópticas tienen una atenuación mínima, debido a las características propias de los materiales (vidrio de cuarzo). Los rangos de longitudes de onda para los que las atenuaciones son mínimas se conocen como “Ventanas”. Las más comunes son las centradas en los 850nm (nano metros), en los 1.300nm y en los 1550nm.

La siguiente figura muestra la atenuación de un cable de fibra óptica en función de la longitud de onda de la luz, y como la evolución tecnológica ha mejorado la atenuación, al punto que casi no se distinguen ya las “ventanas”.

Los emisores ópticos son elegidos de manera que emitan en alguna de las “ventanas”.

**Ancho espectral.** Cuando un transmisor emite luz, la potencia emitida total se distribuye en un rango de longitudes de onda centrados en la “longitud de onda central”. Este rango se conoce como ancho espectral, y depende de las características del emisor. Los láser tienen anchos espectrales más

pequeños que los LEDs, por lo que pueden concentrar mayor potencia en las cercanías de la longitud de onda central, dónde es mínima la atenuación de la fibra.

**Potencia media.** La potencia media de un emisor está directamente relacionada con la intensidad de la luz durante la modulación. Se mide en mW (mili-watts) o dBm. Cuanto mayor sea la potencia media, mayor podrá ser la longitud de la fibra.

**Frecuencia de Modulación.** La frecuencia de modulación de un emisor es la frecuencia a la que la luz puede ser encendida y apagada. La velocidad de transmisión de datos sobre la fibra está limitada por este factor. Para mejorarlo, algunos emisores no llegan a apagar y encender la fuente de luz, sino a cambiar su intensidad, ya que éste puede hacerse más rápidamente.

**Receptores ópticos**

Los receptores ópticos convierten la luz recibida en señales eléctricas. El receptor más comúnmente utilizado es el que se conoce como PIN (photo – intrinsic – negative).

Los receptores ópticos utilizados en un enlace de fibra deben trabajar en la misma ventana (misma longitud de onda) que los emisores. La sensibilidad óptica de los receptores está limitada a la ventana para la que fue diseñado, por lo tanto un receptor diseñado para, por ejemplo, 1300nm, no funcionará correctamente con un emisor de 850nm.

Los receptores ópticos son categorizados según las siguientes características básicas:

- **Sensibilidad.** La sensibilidad de un receptor establece, para una distancia de fibra determinada, la potencia mínima necesaria en el emisor para que pueda ser recuperada correctamente la señal.
- **Tasa de errores (BER=Bit Error Rate).** Durante la conversión de la señal óptica a la eléctrica, pueden producirse errores. La tasa de errores de un receptor es el porcentaje de bits detectados erróneamente. Si la señal recibida es menor a la sensibilidad del receptor, la tasa de errores será grande.
- **Rango dinámico.** Si la potencia transmitida por el emisor es muy baja para la sensibilidad del receptor, la tasa de errores será muy elevada. Sin embargo, si la potencia del emisor es demasiado alta, la tasa de errores también será elevada, ya que el receptor recibirá señales distorsionadas. La diferencia entre los niveles de potencia máximos y mínimos para los que el receptor funciona correctamente se denomina “rango dinámico”.

**Cables de Fibra Óptica**

Los cables de fibra óptica pueden ser descritos como guías de onda para la luz. Son construidos con un núcleo de vidrio (o plástico para aplicaciones de distancias cortas) rodeado de un revestimiento también de vidrio (“cladding”) con índice de refracción menor al núcleo.

Las fibras ópticas se categorizar en dos grupos:

**Fibras Multimodo.** La luz viaja dentro del núcleo de la fibra como una onda dentro de una guía de ondas. Las “ventanas” (longitudes de onda) y los materiales de las fibras se han elegido de manera que la luz forme “ondas estacionarias” dentro de la fibra.

En fibras en las que el núcleo es suficientemente grande (del orden de los 50 μm) pueden existir varias ondas estacionarias, cada una en un “modo” de oscilación. Este tipo de fibras se conocen como “**multimodo**”.

Existen dos tecnologías de fabricación para este tipo de fibras. En la primera, hay una clara separación entre el núcleo y el cladding, como se muestra en la siguiente figura. El diámetro del núcleo está perfectamente determinado, y es del orden de los 50 μm. Este tipo de fibras se conocen como “Step Index”.

Es de notar que en este tipo de fibras, la luz puede transitar por caminos de distinta longitud total (de acuerdo a cada uno de los “modos”). La velocidad de propagación de la luz dentro del núcleo está dada por

$$\mathbf{v = c / n_1}$$

siendo **c** la velocidad de la luz, y $\mathbf{n_1}$ el índice de refracción del núcleo. Dado que la luz siempre está confinada dentro del núcleo, la velocidad es la misma para todos los modos. Como cada modo recorre caminos diferentes, fotones que ingresaron en forma simultánea a la entrada de la fibra pueden salir en momentos diferentes, dependiendo del camino (modo) que hayan seguido. Esto produce dispersión, tal como se ve en la figura, dónde al ingresar un impulso de luz “rectangular”, a la salida el impulso de luz se ve “redondeado”.

Esta dispersión (conocida como “dispersión modal”) limita el ancho de banda utilizable de la fibra óptica.

Para mejorar esta situación, es posible fabricar fibras ópticas de “índice gradual”. En estas fibras, el índice de refracción cambia en forma gradual, desde el núcleo hasta el cladding. De esta manera, la cuando un rayo de luz se aleja del centro del núcleo hacia el cladding, el índice de refracción cambia (disminuye) gradualmente, curvando el rayo de luz hasta hacerlo “volver” hacia el centro. Dado que la velocidad de propagación depende del índice de refracción, en los momentos en los que la luz se encuentra más alejada del núcleo, se desplaza más rápido. Esto compensa la diferencia de tiempos de los distintos “modos”, disminuyendo por lo tanto la dispersión modal y aumentando el ancho de banda utilizable de la fibra.

Las fibras multimodo comerciales se conocen generalmente por el diámetro del núcleo y el cladding. Las más comunes son 50/125 µm y 62.5/125 µm.

Las ventanas utilizadas en las fibras multimodo son las de 850 nm y 1300 nm, con emisores del tipo LED.

**Fibras Monomodo.** Las fibras monomodo se diferencias de las multimodo esencialmente en el diámetro del núcleo. A diferencia de las multimodo, que tienen núcleos del orden de los 50 µm, los núcleos de las fibras monomodo son de 8 a 9 µm.

Estos diámetros tan pequeños no permiten que la luz viaje en varios “modos”, sino que solo puede existir un camino dentro del núcleo. Al existir

únicamente un modo, la dispersión modal es mínima, lo que permite tener un gran ancho de banda aún a distancias grandes.

Las fibras monomodo comerciales tienen diámetros de 9/125 µm. Las ventanas utilizadas son las de 1300nm y 1550nm, con emisores del tipo laser.

Dado que las fibras monomodo son más caras que las multimodo, al igual que los emisores requeridos, su uso se restringe generalmente a aplicaciones de grandes distancias (más de 50km), siendo rara vez utilizadas dentro de edificios.

**Factores que afectan la performance de los sistemas ópticos**

Los factores más comunes que afectan la performance de los sistemas ópticos son los siguientes:

**Atenuación.** Es la diferencia de potencias entre la señal emitida y la recibida. Las razones principales de la atención son la dispersión y la absorción. El vidrio tiene propiedades intrínsecas que causan la dispersión de la luz. La absorción es causa por impurezas que absorben determinadas longitudes de onda.

Otros factores que aportan a la atención son el micro y el macro curvaturas, causadas generalmente por malas prácticas de instalación o conectorización.

**Ancho de Banda.** El ancho de banda de una fibra óptica es un resultado directo de la dispersión. La dispersión causa que los pulsos de luz se “ensanchen” en su duración a medida que atraviesan la fibra.

Existen 3 tipos de dispersión:

En las fibras multimodo, la dispersión modal se debe a que cada modo de propagación dentro de la fibra recorre longitudes diferentes, atrasando por lo tanto a la luz que recorre los caminos más largos. El efecto es menor en las fibras de índice gradual, pero también existe.

La dispersión cromática se debe a que la velocidad de la luz dentro del vidrio depende también de la longitud de onda. La dispersión por esta causa depende directamente del ancho espectral del emisor, siendo mayor para los LEDs que para los laser.

La dispersión de guía de onda se debe a que parte de la luz viaja por el cladding, y es especialmente notorio en las fibras monomodo (en las que los otros dos factores son mínimos).

El ancho de banda se mide en “MHz – km”. Por ejemplo, un ancho de banda de 200 MHz-km indica que la fibra puede transportar una señal de 200 MHz hasta una distancia de 1km, una señal de 100 MHz hasta 2km, una señal de 50 MHz hasta 4km, etc.

**Construcción de cables de fibras ópticas**

Durante el proceso de manufacturación, las fibras son recubiertas con una protección de 250 µm, que cubre al conjunto núcleo/cladding. Esta protección le brinda a la fibra óptica la fortaleza mínima necesaria para su uso en aplicaciones de telecomunicaciones. Sobre esta protección, a su vez, se aplica un recubrimiento, que puede ser de dos tipos:

**Fibras de “tubos sueltos” (“Loose-tube”)**

En este tipo de cables, la fibra con su protección de 250 µm queda “suelta” dentro de un recubrimiento plástico. Esto permite a la fibra cierta

movilidad, necesaria cuando el cable se expone a variaciones de temperaturas importantes, dado que los coeficientes de dilatación de la fibra no pueden ser iguales a los del recubrimiento. Si la fibra se dejara firmemente pegada al recubrimiento, los diferentes coeficientes de dilatación podrían causar fisuras en la fibra.

Este tipo de cables se utiliza generalmente para exteriores, cuando el cable se expone a cambios de temperaturas importantes, entre el día y la noche o entre las estaciones.

A su vez, este tipo de cables puede tener recubrimiento metálico (se llama “cable armado”) o ser completamente dieléctrico.

El cable armado es ideal para instalaciones directamente enterradas, ya que brinda protección anti roedores. El cable completamente dieléctrico es ideal para usos aéreos o para instalaciones dentro de ductos, ya que puede ser instalado cerca de cables de potencia, sin riesgo de corrientes inducidas, y a su vez no afectan a los caminos de descarga ante la caída de rayos.

**Fibras de “recubrimiento ajustado” (“Tight Buffered”).**

En este tipo de cables, la fibra con su protección de 250 µm queda recubierta por una protección plástica de unos 900 µm. Es más sensible a los cambios de temperatura, por lo que este tipo de cables se utiliza generalmente en interiores de edificios. Asimismo, es más fácil de manipular y conectorizar.

**Características de transmisión**

Según el estándar ANSI/TIA/EIA 568-B.3 Las cables de fibra óptica deben cumplir con los siguientes requerimientos:

| Tipo de cable | Longitud de onda | Máxima atenuación (dB/km) | Mínima capacidad de transmisión de información (MHz . km) |
|---|---|---|---|
| Multimodo de 50/125 µm | 850 | 3.5 | 500 |
| | 1300 | 1.5 | 500 |
| Multimodo de 62.5/125 µm | 850 | 3.5 | 160 |
| | 1300 | 1.5 | 500 |
| Monomodo de interior | 1310 | 1.0 | N/A |
| | 1550 | 1.0 | N/A |
| Monomodo de interior | 1310 | 0.5 | N/A |
| | 1550 | 0.5 | N/A |

***Figura Nº 48 Características de Transmisión Vía Fibra Óptica***

**Características Físicas**

Las cables de fibra óptica admitidos por ANSI/TIA/EIA 568-B.3 son multimodo de 50/125 µm y 62.5/125 µm y fibras monomodo.

Los cables para interiores deben soportar un radio de curvatura de 25 mm. Los cables de 2 o 4 hilos de interior, al momento de tenderlos, deben soportar una radio de curvatura de 50mm bajo una tensión de 222 N (50lbf). Todos los cables deben soportar un radio de curvatura de 10 veces el diámetro externo del cable sin tensión y 15 veces el diámetro externos bajo la tensión de tendido.

Los cables para exterior deben tener protección contra el agua y deben soportar una tensión de tenido mínima de 2670 N (600lbf). Todos los cables de exterior deben soportar un radio de curvatura de 10 veces el diámetro externo del cable sin tensión y 20 veces el diámetro externos bajo la tensión de tendido

**Conectores**

De acuerdo al estándar ANSI/TIA/EIA 568-B.3, los conectores para fibras multimodo deben ser de color beige. Los conectores para fibras monomodo deben ser de color azul.

El estándar tomo como ejemplo el conector 568SC, pero admite cualquier otro que cumpla las especificaciones mínimas.

Los conectores de fibra utilizan 2 “hilos” de fibra (ya que la transmisión sobre fibra es generalmente unidireccional. Cada hilo de fibra se termina en un conector, que deben estar claramente marcados como “A” y “B” respectivamente.

Las cajas de conexión de fibra en las áreas de trabajo deben tener como mínimo 2 conectores, y deben permitir un radio de curvatura mínimo de 25 mm.

Los cordones de interconexión (o patch-cords) de fibra pueden ser dobles (es decir, de 2 hilos) o simples.

Los conectores de los extremos de los cables de fibra no deben atenuar más de 0.75 dB

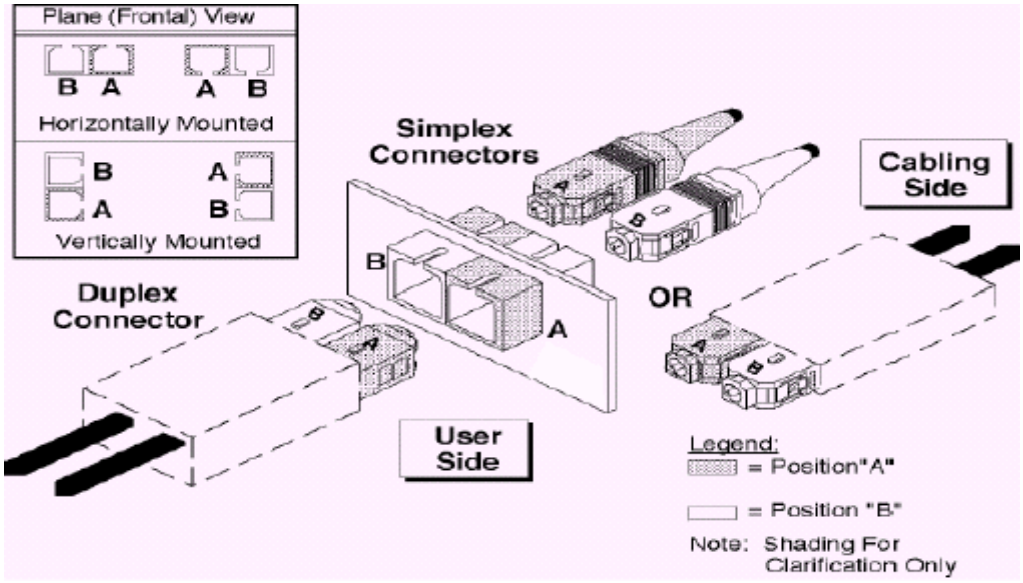



***Figura Nº 49 Conectores y adaptadores para Fibra Óptica***

**Empalmes**

El estándar ANSI/TIA/EIA 568-B.3 admite empalmes de fibra por fusión o mecánicos. En cualquiera de los casos, cada empalme no debe atenuar más de 0.3 dB

## 4.6 MEDIOS DE TRANSMISIÓN

El propósito de la capa física es transportar una corriente de bits en bruto de una máquina a otra. Se pueden usar varios medios físicos para la transmisión real; cada uno con su propio nicho en términos de ancho de banda, retardo, costo y facilidad de instalación y mantenimiento. A grandes rasgos, los medios se agrupan en medios guiados, como el cable de cobre y la fibra óptica, y medios no guiados, como la radio y los láseres a través del

### 4.6.1 Medio Alámbrico

**Fibra Óptica**

El ancho de banda asequible en el caso de la fibra es enorme. El límite práctico de señalización actual de cerca de 1Gbps se debe a la incapacidad para convertir con mayor rapidez las señales eléctricas a ópticas. En el laboratorio, es factible obtener 100Gbps en transmisiones cortas. Los sistemas totalmente ópticos, que incluyen entradas y salidas ópticas de la computadora, están al alcance.

Un sistema de transmisión óptico tiene tres componentes: la fuente de luz, el medio de transmisión y el detector. Convencionalmente, un pulso de luz indica un bit 1 y la ausencia indica un bit 0. El medio de transmisión es una

fibra de video ultradelgada. El detector genera un pulso eléctrico cuando la luz incide en él. Al conectar una fuente de luz en un extremo de una fibra óptica y un detector en el otro, tenemos un sistema de transmisión de datos unidireccional que acepta una señal eléctrica, la convierte y la transmite por pulsos de luz, y después reconvierte la salida de una señal eléctrica en el extremo receptor.

Este sistema de transmisión tendría fugas de luz y sería inútil en la práctica excepto por un principio interesante de la física. Cuando un rayo de luz pasa de un medio a otro, el rayo se refracta (se dobla. El grado de refracción depende de las propiedades de los dos medios (en particular, de sus índices de refracción). Para algunos ángulos de incidencia por encima de cierto valor crítico, la luz se refracta. Así, un rayo incidente con un ángulo igual o mayor que el crítico queda atrapado dentro de la fibra, y se puede propagar por muchos kilómetros virtualmente sin pérdidas.

Para las comunicaciones se utilizan tres bandas de longitud de onda, las cuales se centran respectivamente en 0.85, 1.30 y 1.55 micras. Las últimas dos tienen buenas propiedades de atenuación. La banda restante tiene una atenuación más alta pero la propiedad conveniente de que a esa longitud de onda los láseres y los componentes electrónicos se pueden fabricar con el mismo material.

La longitud de los pulsos de luz transmitidos por una fibra aumenta conforme se propagan.

Este fenómeno se llama **dispersión**, y su magnitud depende de la longitud de onda. Una forma de evitar que se encimen los pulsos dispersos es incrementar la distancia entre ellos, pero esto solamente se puede hacer

reduciendo la velocidad de emisión de las señales. Por fortuna, se ha descubierto que al dar a los pulsos cierta forma especial (relacionada con el recíproco del coseno hiperbólico), todos los efectos de la dispersión se cancelan y puede ser posible enviar pulsos a miles de kilómetros sin una distorsión apreciable de la forma.

Los cables de fibra óptica son similares a los coaxiales, excepto por el trenzado. El núcleo de vidrio está al centro, y a través de él se propaga la luz. En las fibras multimodales el diámetro es de 50 micras. En las fibras monomodo el núcleo es de 8 a 10 micras. El núcleo está rodeado por un revestimiento de vidrio con un índice de refracción menor que el núcleo, a fin de mantener toda la luz en el núcleo. A continuación viene una cubierta plástica delgada para proteger al revestimiento.

Las fibras normalmente se agrupan en haces, protegidas por una funda exterior.

Se pueden utilizar dos clases de fuente de luz para producir las señales, LED (diodos emisores de luz) y láseres semiconductores.

El extremo receptor de una fibra óptica consiste en un fotodiodo que emite un pulso eléctrico cuando lo golpea la luz. El tiempo de respuesta normal de los fotodiodos es de 1ns, lo que limita la velocidad de datos a cerca de 1Gbps. El ruido térmico es otro inconveniente, por lo que un pulso de luz debe llevar energía suficiente para ser detectable.

**Cable UTP**

El medio de transmisión más viejo y todavía más común es el **par trenzado**. Un par trenzado consiste en dos alambres de cobre aislados. Los alambres se trenzan en forma helicoidal.

El propósito de torcer los alambres es reducir la interferencia eléctrica de pares similares cercanos.

Se pueden tener varios kilómetros de par trenzado sin necesidad de amplificación, pero se necesitan repetidores para distancias mayores. Cuando muchos pares entrelazados corren distancias sustanciales en paralelo, se atan en un haz y se forran con una funda que los protege.

Los pares trenzados se pueden usar tanto para transmisión analógica como digital. El ancho de banda depende del grosor del cable y de la distancia, pero en muchos casos se pueden lograr varios Mbps durante algunos kilómetros. Los pares trenzados se usan ampliamente debido a su rendimiento adecuado y a su bajo costo, y no parece que esto vaya a cambiar durante algunos años.

El cableado de par trenzado tiene algunas variaciones, dos de las cuales son importantes para las redes de computadoras. Los pares entrelazados de la **categoría 3** consisten en dos hilos aislados que se trenzan de manera delicada. Cuatro de estos pares se agrupan por lo regular en una funda de plástico para su protección y para mantener juntos los ocho hilos. Por otro lado, los pares trenzados más avanzados de la **categoría 5**; son similares a los de categoría 3, pero con más vueltas por centímetro y con aislamiento de teflón, lo cual produce menor diafonía y una señal de mejor calidad a distancias más

largas, lo que los hace más adecuados para la comunicación de computadoras a alta velocidad. Ambos tipos de cableado con frecuencia reciben el nombre de **UTP** (*Unshielded Twisted Pair*, **par trenzado sin blindaje**).

### 4.6.2 Medios Inalámbricos

Al conectarse una antena del tamaño apropiado a un circuito eléctrico, las ondas electromagnéticas se pueden difundir de manera eficiente y captarse por un receptor a cierta distancia.

Las porciones de radio, microondas, infrarrojo y luz visible del espectro pueden servir para transmitir información modulando la amplitud, la frecuencia o la fase de las ondas. La luz ultravioleta, los rayos X y los rayos gamma serían todavía mejores, debido a sus frecuencias más altas, pero son difíciles de producir y de modular, no se propagan bien entre edificios y son peligrosos para los seres vivos.

#### Radiotransmisión

Las ondas de radio son fáciles de generar, pueden viajar distancias largas y penetrar edificios sin problemas, de modo que se utilizan mucho en la comunicación, tanto en interiores como en exteriores. Las ondas de radio también son omnidireccionales, lo que significa que viajan en todas direcciones desde la fuente, por lo que el transmisor y el receptor no tienen que alinearse físicamente.

Las propiedades de las ondas de radio dependen de la frecuencia. A bajas frecuencias, las ondas de radio cruzan bien los obstáculos, pero la potencia se reduce drásticamente con la distancia a la fuente. A altas

frecuencias, las ondas de radio tienden a viajar en línea recta y a rebotar en los obstáculos. También son absorbidas por la lluvia. En todas las frecuencias, las ondas de radio están sujetas a interferencia por equipos eléctricos de diverso índole.

### Transmisión por microondas

Por encima de los 100 MHz las ondas viajan en línea recta y, por tanto, se pueden enfocar en un haz estrecho. Concentrar toda la energía en un haz pequeño con una antena parabólica produce una señal mucho más alta en relación con el ruido, pero las antenas transmisora y receptora deben estar muy bien alineadas entre sí. Además, esta direccionalidad permite que múltiples transmisores alineados en una fila puedan comunicarse con múltiples receptores en fila, sin interferencia.

Ya que las microondas viajan en línea recta, si las torres están muy alejadas, la superficie terrestre puede llegar a molestar. En consecuencia, se necesitan repetidoras periódicas. Cuantas más altas sean las torres, más separadas pueden estar.

A diferencia de las ondas de radio a frecuencias más bajas, las microondas no atraviesan bien los edificios. Además, aun cuando el haz puede estar bien enfocado en el transmisor, hay cierta divergencia en el espacio. Algunas ondas pueden refractarse en las capas atmosféricas más bajas y tardar un poco más en llegar que las ondas directas. Las ondas diferidas pueden llegar fuera de fase con la onda directa y cancelar así la señal. Este efecto se llama **desvanecimiento por trayectoria múltiple** y con frecuencia es un problema serio que depende del clima y de la frecuencia.

Las microondas son relativamente baratas y, por esta razón, se utilizan tanto para la comunicación telefónica de larga distancia, los teléfonos celulares, la distribución de la televisión y otros usos.

## 4.7 INTRANET

### 4.7.1 Generalidades

Una Intranet es un conjunto de aplicaciones internas de la empresa para uso exclusivo de sus empleados. Estas aplicaciones pretenden mejorar el desempeño individual de cada empleado y mejorar la productividad general de la empresa, reduciendo costos y aumentando el tiempo productivo de cada empleado.

Una Extranet no es más que brindar acceso a ciertas aplicaciones o información de la Intranet a proveedores, empresas, personas, etc. que la empresa desee.

Las Intranets son un campo aún muy nuevo, pero su uso está creciendo aún más rápido que la propia Internet. Según estimaciones recientes, cada cuatro minutos se abre en algún lugar del mundo una instalación de este tipo.
Una Intranet y en particular cada una de sus aplicaciones, brinda una serie de beneficios a la empresa que le permiten alcanzar sus objetivos más fácilmente.

En general 2 de los principales beneficios son:

- Reducir el tiempo desaprovechado en tareas operativas manuales que pueden ser automatizadas, de esta forma los empleados pueden dedicar su tiempo a tareas que brinden un mayor valor a la empresa.

- Reducción de costos: que se obtiene al sistematizar procesos que actualmente utilizan recursos costosos (como papel, tinta, etc.) y que pueden ser incorporados a la Intranet y manejados de forma digital. No obstante, ninguna Intranet es realmente típica. Las personas utilizan la tecnología para diferentes cosas. Hay tantas aplicaciones de Intranets como tipos de organizaciones y tipos de negocios existen. Lo importante es ver de qué forma se puede potencializar su uso dentro de la empresa.

La plataforma también puede ser muy distinta, siempre que estemos trabajando sobre TCP/IP internamente podemos hablar que se trata de nuestra Intranet. El concepto incluye el uso del “browser” o navegador de Web (Internet Explorer o Netscape) como la interfase de información. Algunas de las ventajas del uso de esta interface son:

- Reduce el tiempo de aprendizaje de los usuarios.
- Simplifica la instalación de aplicaciones.
- Presenta diferentes tipos de información: texto, gráficas, sonido y video.
- Actúa como "front-end" para las aplicaciones cliente-servidor.
- Permite el acceso a bases de datos.

### 4.7.2. Objetivos de una intranet

- Mejorar los canales de comunicación dentro de la organización.
- Compartir recursos informativos y formativos
- Compartir recursos informáticos y utilidades

- Crear una comunidad virtual.
- Facilitar el trabajo de los usuarios de la red
- Establecer una infraestructura para la explotación de aplicaciones internas
- El usuario no necesita formación para adecuarse a esta plataforma por que totalmente weboriented

**Usos y Aplicaciones**

En general las aplicaciones que pueden generarse para una Intranet deben cumplir con cualquiera de las siguientes características:

- Cualquier proceso interno de la empresa que al momento se realice utilizando papel es susceptible de ser migrado a la Intranet con el consiguiente ahorro en costos y tiempo. (Ej.: directorio de empleados, descripción de beneficios médicos, listas de precios, políticas y procedimientos, etc.)
- Cualquier proceso que involucre consolidación de información de muchas fuentes de datos (Ej. reportes de ventas, etc.)
- Cualquier proceso que requiera un alto nivel de comunicación y colaboración entre las personas.
- Cualquier proceso que requiera encontrar/solicitar información (Ej. manuales, información de productos, etc.)

Pero a la vez plantea una nueva forma de relacionarse entre todos los actores de la empresa: tanto internos como externos. Cuando al concepto de Intranet le añadimos el de “Workflow” tenemos un combinado muy interesante que potenciará la vida de la empresa.

En cada área de la empresa se le puede sacar partido. Sin ser exhaustivos, a continuación se expone una lista de posibles aplicaciones de Intranet según departamentos.

**Mercadeo y Ventas:** las Intranets permiten la frecuente adición y actualización de materiales de Ventas y Mercadotecnia, como respuesta a un ambiente de negocios competitivo y dinámico. Una Intranet bien organizada para Ventas y Mercadotecnia puede ayudar a eliminar el exceso de información duplicada: permite resolver las necesidades de los representantes de ventas, quienes necesitan acceso instantáneo a información específica, sin leer grandes cantidades de material impreso.

**Recursos Humanos:** La información de Recursos Humanos, debido a la gran cantidad de papeles y gráficas, se puede usar en una Intranet. La Intranet podría también administrar el reclutamiento, promoción, salarios y asistencias de los empleados, ahorrado gran tiempo y dinero de Recursos Humanos. Además da a los empleados rápido acceso a información de su interés como: Manuales y procedimientos, Políticas, Programas de beneficios, Descripción de puestos, Preguntas frecuentes, Calendarios de vacaciones y días de descanso. Y un largo etcétera.

**Operación y Administración:** Una Intranet puede ayudar a simplificar una variedad de operaciones y funciones administrativas. Una forma de utilizarla es crear una página central donde publicar gráficas, listas de contactos, boletines, preguntes frecuentes, procedimientos, formas,

calendarios, proyectos, aprobaciones en líneas, etc. Otras cosas que se pueden manejar: Información para Empleados, Políticas y Procedimientos, Facilidades, Administración de Ordenes de Venta, Compras, Administración de Contratos, Control de Envíos.

**Finanzas y Jurídicos:** Una Intranet ayuda a los departamentos de finanzas y jurídico para monitorear el estado de los proyectos, llevar un registro de su contabilidad y facturación, y comunicar esta información a toda la empresa. También sirve para almacenar la información extraída de Internet o bases de datos relacionadas al departamento. Entre los principales usos de la Intranet en estos departamentos de la empresa, podemos encontrar: Administración de Contratos, Biblioteca legal electrónica, Aprobaciones, Funciones de Contabilidad y Facturación, Declaraciones de Impuestos, Manejo de cuentas, Presupuestos y Pronósticos, Reportes, Preguntas frecuentes, etc.

**Manufactura:** Los principales usos de la Intranet en Manufactura son: Boletines de Mercado, Kits de Ventas, Cambios en Productos, Presentaciones, Guías de Ventas, Información de Clientes, Listas de Precios, Preguntas Frecuentes, Formas, Especificaciones de Productos, Información de la Competencia, Propuestas, Listas de Contactos, Encuestas y Reportes, Información de Distribuidores, Información Miscelánea

**Algunos Problemas**

Aunque la construcción de herramientas sobre Intranets ha crecido mucho en las grandes empresas y la tendencia continúa aún a la alza, se

empiezan a ver algunos inconvenientes. En la mayor parte de las encuestadas nos hemos encontrado con que no todas son buenas noticias. Existen varios problemas puntuales: **falta de capacitación** del personal para el uso correcto de la herramienta; **información desactualizada**; **poco uso** de la herramienta; **escaso apoyo directivo** en el crecimiento e implementación adicional de nuevas fases más interactivas; etc. No se tienen datos registrados sobre el uso de las Intranets en las pymes, pero podemos imaginarnos que muchas tendrán que luchar con los mismos problemas. Poco desarrolladas y desaprovechadas, a las Intranets se les presta escasa atención. Pero la tendencia cambia cuando las empresas descubren lo útiles que pueden resultar.

Desarrollar una Intranet es un proceso sencillo, requiere poca preparación y pocos recursos. Pero diseñar una estrategia que se apoye en la Intranet que apalanque la operación de la empresa ayudándola a conseguir sus metas, eso es harina de otro costal. Bien planificadas, las Intranets ahorran tiempo y dinero a la empresa Hay que potenciar su uso dentro de la empresa: esta es la misión de los gerentes de sistemas, apoyados por compañías consultoras expertas en el tema.

La falta de definiciones claras conduce a muchos a hacer inversiones poco inteligentes en sus Intranets, que no convence a los directivos y frena los posibles desarrollos que a futuro se podrían implementar: una mala experiencia en un desarrollo temprano puede significar el fin de una herramienta que bien pensada, pudo haber traído muchos beneficios. La Intranet es un gran aliado, pero **si no se planifican** con visión estratégica **pueden morir** por esos dos males: poca eficacia o poco uso.

### 4.7.3. Desarrollo de la Intranet

Una Intranet es una red privada que la tecnología Internet usó como arquitectura elemental. Una red interna se construye usando los protocolos TCP/IP para comunicación de Internet, que pueden ejecutarse en muchas de las plataformas de hardware y en proyectos por cable. El hardware fundamental no es lo que construye una Intranet, lo que importa son los protocolos del software. Las Intranets pueden coexistir con otra tecnología de red de área local. En muchas compañías, los "sistemas patrimoniales" existentes que incluyen sistemas centrales, redes Novell, mini - computadoras y varias bases de datos, se están integrando en un Intranet. Una amplia variedad de herramientas permite que esto ocurra.

Con el enorme crecimiento de Internet, un gran número de personas en las empresas usan Internet para comunicarse con el mundo exterior, para reunir información, y para hacer negocios. A la gente no le lleva mucho tiempo reconocer que los componentes que funcionan tan bien en Internet serían del mismo modo valioso en el interior de sus empresas y esa es la razón por la que las Intranets se están haciendo tan populares. Algunas corporaciones no tienen redes TCP/IP: el protocolo requerido para acceder a los recursos de Internet. Crear una Intranet en la que todas las informaciones y recursos se puedan usar sin interrupciones tiene muchos beneficios. Las redes basadas en TCP/IP facilitan las personas el acceso a la red remotamente, desde casa o mientras viajan. Contactar con una Intranet de este modo es muy parecido a conectar con Internet, la operabilidad interna entre redes es otro suplemento sustancial. Los sistemas de seguridad separan una Intranet de Internet. La red interna de

una compañía está protegida por firewall: combinaciones de hardware y software que sólo permiten a ciertas personas acceder a ella para propósitos específicos. Se puede utilizar para cualquier cosa para la que se empleaban las redes existentes.

Las Intranets permiten a los usuarios trabajar juntos de un modo más sencillo y efectivo. EL programa conocido como trabajo en grupo es otra parte importante de las redes internas. Nos permite colaborar en proyectos, compartir información, llevar a cabo conferencias visuales, y establecer procedimientos seguros para el trabajo de producción. EL software del servidor y del cliente gratuito y la multitud de servicios como los grupos de noticias, estimulan la expansión de Internet. La consecuencia de ese crecimiento avivó y provocó el desarrollo de las Intranets.

**UNA VISION GLOBAL DE UNA INTRANET**

Una Intranet es una red privada empresarial o educativa que utiliza los protocolos TCP/IP de Internet para su transporte básico. Los protocolos pueden ejecutar una variedad de Hardware de red, y también, pueden coexistir con otros protocolos de red, como IPX. Aquellos empleados que están dentro de una Intranet pueden acceder a los amplios recursos de Internet, pero aquellos en Internet no pueden entrar en la Intranet, que tiene acceso restringido.

Una Intranet se compone frecuentemente de un número de redes diferentes dentro de una empresa que se comunica con otra mediante TCP/IP. Estas redes separadas se conocen a menudo como sub - redes. El software que permite a la gente comunicarse entre ella vía e-mail y tablones de mensaje públicos, y colaborar en la producción usando software de grupos de trabajo,

está entre los programas de Intranets más poderoso. Las aplicaciones que permiten a los distintos departamentos empresariales enviar información, y a los empleados rellenar formularios de la empresa (como las hojas de asistencia) y utilizar la información corporativa financiera, son muy populares. La mayoría del software que se utiliza en las Intranets es estándar: software de Internet como el Netscape, Navigator y los navegadores Explorer para Web de Microsoft. Y los programas personalizados se construyen frecuentemente usando el lenguaje de programación de Java.

Las Intranets también se pueden utilizar para permitir a las empresas llevar a cabo transacciones de negocio a negocio como: hacer pedidos, enviar facturas, y efectuar pagos. Para mayor seguridad, estas transacciones de Intranet a Intranet no necesitan nunca salir a Internet, pero pueden viajar por líneas alquiladas privadas. Son un sistema poderoso para permitir a una compañía hacer negocios en línea, por ejemplo, permitir que alguien en Internet pida productos. Cuando alguien solicita un producto en Internet, la información se envía de una manera segura desde Internet a la red interna de la compañía, donde se procesa y se completa el encargo. La información enviada a través de una Intranet alcanza su lugar exacto mediante los enrutadores, que examinan la dirección IP en cada paquete TCP/IP y determinan su destino. Después envía el paquete al siguiente direccionado. Si este tiene que entregarse en una dirección en la misma subred de la Intranet desde la que fue enviado, llega directamente sin tener que atravesar otro enrutador. Si tiene que mandarse a otra subred de trabajo en la Intranet, se enviará a otra ruta. Si el paquete tiene que alcanzar un destino externo a la

Intranet a la Intranet en otras palabras, Internet se envía a un enrutador que conecte con Internet.

Para proteger la información corporativa delicada, y para asegurar que los piratas no perjudican a los sistemas informáticos y a los datos, las barreras de seguridad llamadas firewalls protegen a una Intranet de Internet. La tecnología firewall usa una combinación de enrutadores, servidores y otro hardware y software para permitir a los usuarios de una Intranet utilizar los recursos de Internet, pero evitar que los intrusos se introduzcan en ella. Mucha Intranets tienen que conectarse a "sistemas patrimoniales": el hardware y las bases de datos que fueron creadas antes de construir la Intranet. A menudo los sistemas patrimoniales usan tecnologías más antigua no basada en los protocolos TCP/IP de las Intranets. Hay varios modos mediante los que las Intranets se pueden unir a sistemas patrimoniales.

**COMO FUNCIONA TCP/IP E IPX EN LAS INTRANETS**

Lo que distingue una Intranet de cualquier otro tipo de red privada es que se basa en TCP/IP: los mismos protocolos que se aplican a Internet. TCP/IP se refiere a los dos protocolos que trabajan juntos para transmitir datos: el Protocolo de Control de Transmisión (TCP) y el Protocolo Internet (IP). Cuando envías información a través de una Intranet, los datos se fragmentan en pequeños paquetes. Los paquetes llegan a su destino, se vuelven a fusionar en su forma original. El Protocolo de Control de Transmisión divide los datos en paquetes y los reagrupa cuando se reciben. El Protocolo Internet maneja el encaminamiento de los datos y asegura que se envían al destino exacto.

En algunas empresas, puede haber una mezcla de Intranets basadas en TCP/IP y redes basadas en otra tecnología, como NetWare. En este caso, la tecnología TCP/IP de una Intranet se puede utilizar para enviar datos entre NetWare y otras redes, usando una técnica llamada IP canalizado. Las redes NetWare usan el protocolo IPX(Intercambio de Paquetes en Internet) como medio de entregar datos y las redes TCP/IP no pueden reconocer este protocolo. Cuando un paquete IP mediante un servidor NetWare especifico y que se dedica a ofrecer el mecanismo de transporte del IP para los paquetes IPX.

Los datos enviados dentro de una Intranet deben separase en paquetes menores de 1.500 caracteres. TCP divide los datos en paquetes. A medida que crea cada paquete, calcula y añade un número de control a éstos. El número de control se basa en los valores de los bytes, es decir, la cantidad exacta de datos en el paquete.

Cada paquete, junto al número de control, se coloca en envases IP o "sobre" separados. Estos envases contienen información que detalla exactamente donde se van a enviar los datos dentro de la Intranet o de Internet. Todos los envases de una clase de datos determinada tienen la misma información de direccionamiento así que se pueden enviar a la misma localización para reagruparse.

Los paquetes viajan entre redes Intranets gracias a enrutadores de Intranets. Los enrutadores examinan todos los envases IP y estudian sus direcciones. Estos direccionan determinan la ruta más eficiente para enviar cada paquete a su destino final. Debido a que él trafico en una Intranet cambia frecuentemente, los paquetes se pueden enviar por caminos diferentes y

puedan llegar desordenados. Si el enrutador observa que la dirección está localizada dentro de la Intranet, el paquete se puede enviar directamente a su destino, o puede enviarse a otro enrutador. Si la dirección se localiza fuera de Internet, se enviará a otro enrutador para que se pueda enviar a través de ésta.

A medida que los paquetes llegan a su destino, TCP calcula un número de control para cada uno. Después compara este número de control con el número que se ha enviado en el paquete. Si no coinciden, CP sabe que los datos en el paquete se han degradado durante él envió. Después descarta el paquete y solicita la retransmisión del paquete origina.

TCP incluye la habilidad de comprobar paquetes y determinar que se han recibido todos. Cuando se reciben os paquetes no degradaos, TCP los agrupa en su forma original, unificada. La información de cabecera de los paquetes comunica el orden de su colocación.

Una Intranet trata el paquete IP como si fuera cualquier otro, y envía el paquete a la red NetWare receptora, un servidor TCP/IP NetWare abre el paquete IP descarta el paquete IP, y lee el paquete IPX original. Ahora puede usar el protocolo IPX para entregar los datos en el destino exacto.

**COMO FUNCIONA EL MODELO OSI**

La organización Internacional para la Normalización (ISO) ha creado el modelo de referencia "Interconexión de Sistemas Abiertos" (OSI), que describe siete pilas de protocolos para comunicaciones informáticas. Estas pilas no conocen o no se preocupan de lo que hay en pilas adyacentes. Cada pila, esencialmente, sólo ve la pila recíproca en el otro lado. La pila destinada a enviar la aplicación observa y se comunica con la pila de aplicación en el

destino. Esa conversación tiene lugar sin considerar, por ejemplo, qué estructura existe en la pila física, como Ethernet o Token Ring. TCP combina las pilas de aplicación, presentación y sesión del modelo OSI en una que también se llama pila de aplicación.

**COMO SE PROCESAN LOS PAQUETES TCP/IP**

Los protocolos como TCP/IP determinan cómo se comunican las computadoras entre ellas por redes como Internet. Estos protocolos funcionan conjuntamente, y se sitúan uno encima de otro en lo que se conoce comúnmente como pila de protocolo. Cada pila del protocolo se diseña para llevar a cabo un propósito especial en la computadora emisora y en la receptora. La pila TCP combina las pilas de aplicación, presentación y sesión en una también denominada pila de aplicación.

En este proceso se dan las características del envasado que tiene lugar para transmitir datos:

- La pila de aplicación TCP formatea los datos que se están enviando para que la pila inferior, la de transporte, los pueda remitir. La pila de aplicación TCP realiza las operaciones equivalentes que llevan a cabo las tres pilas de OSI superiores: aplicaciones, presentación y sesión.
- La siguiente pila es la de transporte, que es responsable de la transferencia de datos, y asegura que los datos enviados y recibidos son de hecho los mismos, en otras palabras, que no han surgido errores durante él envió de los datos. TCP divide los datos que obtiene de pila de aplicación en segmento.

Agrega una cabecera contiene información que se usará cuando se reciban los datos para asegurar que no han sido alterados en ruta, y que los segmentos se pueden volver a combinar correctamente en su forma original.

- La tercera pila prepara los datos para la entrega introduciéndolos en data gramas IP, y determinando la dirección Internet exacta para estos. El protocolo IP trabaja en la pila de Internet, también llamada pila de red. Coloca un envase IP con una cabecera en cada segmento. La cabecera IP incluye información como la dirección IP de las computadoras emisoras y receptoras, la longitud del data grama y el orden de su secuencia. El orden secuencial se añade porque el data grama podría sobrepasar posiblemente el tamaño permitido a los paquetes de red, y de este modo necesitaría dividirse en paquetes más pequeños. Incluir el orden secuencial les permitiría volverse a combinar apropiadamente.

**COMO FUNCIONAN LOS PUENTES**

Los puentes son combinaciones de hardware y software que conectan distintas partes de una red, como las diferentes secciones de una Intranet. Conectan redes de área local (LAN) entre ellas. Sin embargo, no se usan generalmente para conectar redes enteras entre ellas, por ejemplo: para conectar una Intranet con Internet; o una Intranet con otra, o para conectar una

subred completa con otra. Para hacer eso, se usan piezas de tecnología más sofisticada llamadas enrutadores.

Cuando hay gran cantidad de tráfico en una red de área local Ethernet, los paquetes pueden chocar entre ellos, reduciendo la eficacia de la red, y atrasando el tráfico de la red. Los paquetes pueden colisionar porque se encamina mucho tráfico entre todas las estaciones de trabajo en la red.

Para reducir la proporción de colisiones, una LAN se puede subdividir en dos o más redes. Por ejemplo, una LAN se puede subdividir en varias redes departamentales. LA mayoría del tráfico en cada red departamental se queda dentro de la LAN del departamento, y así no necesita viajar a través de todas las estaciones de trabajo en todas las LAN de la red. De este modo, se reducen las colisiones. Los puentes se usan para enlazar las LAN. El único tráfico que necesita cruzar puentes es el que navega con rumbo a otra LAN. Cualquier trafico con la LAN no necesita cruzar un puente.

Cada paquete de datos en una Intranet posee más información que la del IP. También incluye información de direccionamiento requerida para otra arquitectura de red básica, como Ethernet. Los puentes comprueban esta información de la red externa y entregan el paquete en la dirección exacta en una LAN.

Los puentes consultan una tabla de aprendizaje que contiene las direcciones de todos los nodos de la red. Si un puente descubre que un paquete pertenece a su LAN, mantiene el paquete en la LAN. Si descubre que la estación de trabajo está en otra LAN, envía el paquete. El puente actualiza constantemente la tabla de aprendizaje a medida que controla y encamina el tráfico.

Los puentes pueden conectar redes de área local de varias formas diferentes. Pueden conectar LAN usando conexiones en serie por líneas telefónicas tradicionales y módems, por líneas ISDN, y por conexiones directas por cable. Las unidades CSU / DSU se usan para conectar puentes con líneas telefónicas mediante conductividad remota.

Los puentes y enrutadores se combinan algunas veces en un solo producto llamado router. Un router ejecuta las tareas de ambos. Si los datos necesitan sólo enviarse a otra LAN en la red o subred, solamente actuará como un puente, entregando los datos basados en la dirección Ethernet. Si el destino es otra red, actuará como un enrutador, examinando los paquetes IP y encaminando los datos basados en la dirección IP.

**COMO FUNCIONAN LOS ENRUTADORES DE LAS INTRANETS**

Los enrutadores son los guardias de tráfico de las Intranets. Se aseguran que todos los datos se envían donde se supone que tienen que ir y de que lo hacen por la ruta más eficaz. Los enrutadores también son herramientas útiles para sacar el mejor rendimiento de la Intranet. Se emplean para desviar el tráfico y ofrecer rutas. Los enrutadores utilizan la encapsulación para permitir el envío de los distintos protocolos a través de redes incompatibles.

Los enrutadores abren el paquete IP para leer la dirección de destino, calcular la mejor ruta, y después enviar el paquete hacia el destino final. Si el destino está en la misma parte de una Intranet, el enrutador enviará el paquete directamente a la computadora receptora. Si el paquete se destina a otra Intranet o subred (o si el destino está en Internet), el enrutador considera

factores como la congestión de tráfico y él numero de saltos – términos que se refiere al número de enrutadores o pasarelas en una ruta dada. El paquete IP lleva consigo un segmento que cuenta los saltos y un enrutador no usará una red que exceda de un número de saltos predeterminado. Las rutas múltiples – dentro de un número aceptable de saltos, son convenientes para ofrecer variedad y para asegurar que los datos se pueden transmitir. Por, ejemplo, si una ruta directa entre Madrid y Barcelona no estuviera disponible, los enrutadores sofisticados enviarán los datos a Barcelona por otro enrutador probablemente en otra ciudad en la Intranet, y esto sería transparente para los usuarios.

Los enrutadores tienen dos o más puertos físicos: los de recepción (de entrada) y los de envío (de salida). En realidad, cada puerto es bidireccional y puede recibir o enviar datos. Cuando se recibe un paquete en un puerto de entrada, se ejecuta una rutina de software denominada proceso de encaminamiento. Este proceso investiga la información de cabecera en el paquete IP y encuentra la dirección a la que se están enviando los datos. Luego compara esta dirección con una base de datos llamada tabla de encaminamiento que posee información detallando a que puertos deberían enviarse los paquetes con varias direcciones IP. Basándose en lo que encuentra en la tabla de encaminamiento, envía el paquete en un puerto de salida específico. Este puerto de salida envía después los datos al siguiente enrutador o al destino.

Los paquetes se mandan a un puerto de entrada de un enrutador antes de que pueda procesarlos. Cuando esto ocurre, los paquetes se envían a un área de contención especial llamada cola de entrada, un área de RAM en el

enrutador. Esa cola de entrada específica está asociada con un puerto de entrada concreto. Un enrutador puede tener más de una cola de entrada, si varios puertos de entrada están enviando paquetes más aprisa que el enrutador puede procesarlos. Cada puerto de entrada procesará los paquetes de la cola en el orden en que se recibieron.

Si él tráfico a través del enrutador es muy denso, el número de paquetes en la cola puede ser mayor que su capacidad. (La capacidad de la cola se denomina longitud). Cuando esto ocurre, es posible que los paquetes se abandonen y de este modo no serán procesados por el enrutador, y no se enviarán a su destino. Aunque esto no significa que se tenga que perder la información. El protocolo TCP se diseño para tener en cuenta que los paquetes pueden perderse de camino a su destino final. Si nos envían todos los paquetes al receptor, TCP en la computadora receptora identifica y pide que se vuelvan a enviar los paquetes perdidos. Seguirá solicitando él reenvió de los paquetes hasta que reciban todos. Los enrutadores sofisticados pueden manejarse y los problemas diagnosticarse y resolverse usando software especial, como SNMP (Protocolo Simple de Administración de Red). TCP puede decidir que decisiones tiene que tomar porque hay varias banderas en el paquete, como el número de saltos en IP, que comunica a TCP lo que necesita para saber cómo actuar. Por ejemplo, la bandera ack, indica que esta respondiendo (reconociendo) a una comunicación previa.

Se utilizan varios tipos de tablas en ruta. En el tipo de Intranet más simple denominada tabla de encaminamiento mínimo. Cuando una Intranet se compone de una sola red TCP/IP o a Internet, se puede usar encaminamiento mínimo. En encaminamiento mínimo, un programa llamado ifconfig crea

automáticamente la tabla, que contiene únicamente unas pocas entradas básicas. Puesto que hay muy pocos lugares a los que se pueden enviar los datos, sólo se necesita configurar un número mínimo de enrutadores.

Si una Intranet tiene solamente un número limitado de redes TCP/IP, se puede utilizar una tabla de encaminamiento estático. En este caso, los paquetes con direcciones específicas se envían a enrutadores específicos. Los enrutadores no desvían paquetes para modificar el tráfico variable de la red. El encaminamiento estático debería utilizarse cuando sólo hay una ruta para cada destino. Una tabla de encaminamiento estático permite a un administrador de Intranets añadir o eliminar entradas en ésta.

Las tablas de encaminamiento dinámico son las más sofisticadas. Deberían usarse cuando hay más de una manera para enviar datos desde un enrutador al destino final, y en Intranets más complejas. Estas tablas cambian constantemente a medida que varía el trafico de la red y las condiciones, así que siempre encaminan datos del modo más eficiente posible, teniendo en cuanta el estado actual del tráfico de la Intranet.

Las tablas de encaminamiento dinámico se construyen utilizando protocolos de encaminamiento. Estos protocolos son medios por los que se comunican los enrutadores, ofreciendo información sobre la manera más eficaz de encaminar datos dado el estado actual de la Intranet. Un enrutador con una tabla de encaminamiento dinámico puede desviar datos a una ruta de apoyo si la ruta primaria es reducida. También puede determinar siempre el método más eficiente de encaminar datos hacia su destino final. Los enrutadores exponen sus direcciones IP y conocen las direcciones IP de sus vecinos. Los

enrutadores pueden usar esta información en un algoritmo para calcular la mejor ruta para enviar paquetes.

El protocolo de encaminamiento más común que realiza estos cálculos se conocen como RIP (Protocolo de Información de Encaminamiento). Cuando RIP determina la ruta más eficaz para enviar datos el camino con el menor número de saltos. Asume que cuantos menos saltos haya, más eficaz un número de saltos mayor que 16, descartará la ruta.

El Protocolo de Pasarela Exterior (EGP) se usa en Internet donde se puede tener que atravesar muchos más enrutadores antes de que un paquete alcance su destino final.

El factor a tener en cuenta sobre Intranets y Tecnología de encaminamiento es que no es una situación "o se da una u otra", sino que pueden utilizar muchos tipos de tecnologías de encaminamiento, dependiendo de las necesidades de esa parte particular de la red. Algunas partes pueden ser capaces de emplear enrutadores con tablas de encaminamiento estático, mientras que otras partes pueden necesitar tablas de encaminamiento dinámico.

**COMO SE REPARTE EL EMAIL DENTRO DE UNA INTRANET**

Probablemente la parte más usada de una Intranet que no tiene nada que ver con bases de datos de la empresa, páginas Web ostentosas. O contenido multimedia es el uso del correo electrónico. Las Intranets empresariales pueden emplear diferentes programas e-mail, como cc: Mail Microsoft Mail o Lotus Notes, entre otros. Pero la Arquitectura más común que

sirve de base al uso del e-mail de las redes internas es el protocolo llamado Protocolo simple de Transferencia de Correo, o SMTP.

Como se utiliza SMTP para repartir correo dentro de una Intranet:

- Como sucede con muchas aplicaciones de Intranets y de Internet, SMTP usa una arquitectura cliente / servidor. Cuando alguien quiere crear un mensaje, usa un agente usuario de correo o agente usuario (MUA o UA), software cliente que se ejecuta en un computador, para crear un fragmento de correo electrónico. Este MUA puede ser cualquiera de los programas e-mail, y puede ejecutarse en varias computadoras diferentes, incluyendo PC, Macintosh,, y estaciones de trabajo UNÍS; Pegasus, Eudora. cc: Mail y Microsoft Mail para PC; y Eudora para Macintosh.
- Después de finalizar el mensaje, el MUA lo manda a un programa que s esta ejecutando en un servidor llamado agente de transferencia de correo (MTA) examina la dirección del receptor de mensaje. Si el receptor del mensaje está en la Intranet, el MTA envía el mensaje a otro programa servidor en la red interna denominado agente de entrega de correo (MDA). Si el receptor está ubicado en Internet o en otra red interna, el archivo llegará al receptor a través de Internet. El MDA examina la dirección del receptor, y envía el correo a la bandeja de entrada d el apersona adecuada.
- Algunos sistemas de correo emplean otro protocolo e-mail llamado el Protocolo de Oficina de Correos (POP)

conjuntamente con SMTP. Con POP, el e-mail no se entrega directamente en tu computadora. En lugar de eso, el correo se echa a un buzón en el servidor. Para conseguir el coreo, alguien accede al servidor usando una contraseña y un nombre de usuario, y recupera el mensaje con un agente de correo.

- El receptor del correo puede utilizar ahora un agente usuario de correo para leer el mensaje, archivarlo y responderlo.
- SMTP sólo puede manejar la transferencia de e-mail de archivos de textos ASCII sencillos. Para enviar archivos binarios como hojas de cálculos, dibujos y documentos de procesador de texto, primero deben convertirlos en un formato ASCII codificándolos. Los archivos se pueden codificar usando varios métodos que incluyen codificación y Base64. Algunos software e-mail codificará automáticamente archivos binarios. Cuando alguien recibe un archivo codificado, lo descodifica y después puede usar o examinar el archivo binario. Además muchos paquetes e-mail descodifican automáticamente archivos codificados.

**COMO SE REPARTE E-MAIL ENTRE INTRANETS**

A menudo el e-mail creado en una Intranet no se entregará a una computadora de la Intranet, sino a alguien en Internet, sino a alguien en Internet, en otra Intranet, o un servidor en línea como América Online, Microsoft

Network, o CompuServe. Aquí están los pasos que un mensaje típico tiene que seguir cuando se envía de una Intranet a otra red o Intranet.

Un mensaje e-mail se crea usando SMTP. Como ocurre con toda la información enviada a través de Internet, el mensaje es dividido por el Protocolo TCP de Internet en paquetes IP. La dirección la examina el agente de transferencia de correo de la Intranet. Si la dirección se encuentra en otra red, el agente de transferencia de correo enviará el correo a través de la Intranet mediante enrutadores al agente de transferencia de correo en la red receptora.

Antes de que se pueda enviar el correo a través de Internet, puede que primero tenga que atravesar un firewall, una computadora que protege a la Intranet para que los intrusos no puedan acceder a ella. El firewall sigue la pista de los mensajes y los datos que entran y salen de la Intranet.

El mensaje deja la Intranet y se envía a un enrutador Internet. El enrutador examina la dirección, determina dónde debería mandarse el mensaje, y después lo pone en camino.

La red receptora obtiene el mensaje e-mail. Aquí utiliza una pasarela para convertir los paquetes IP en un mensaje completo. Después la pasarela traduce el mensaje al protocolo particular que emplea la red (como el formato de correo de Compu-Serve), y lo pone en camino. Puede que el mensaje también tenga que atravesar un firewall en la red receptora.

La red receptora examina la dirección e-mail y envía el mensaje al buzón especifico donde el mensaje está destinado a ir, o emplea el Protocolo de Oficina de Correo (POP) para entregarlo a un servidor de correo.

Las pasarelas realmente pueden modificar los datos (si se necesita) para la conectividad. Para el e-mail, puede convertir el protocolo Compu-Serve en

SMTP. Las pasarelas también se utilizan para conectar PC con sistemas centrales IBM, por ejemplo, ASCII con EBCDIC.

**COMO FUNCIONA UNA INTRANET**

El centro de una Intranet es la World Wide Web. En muchos casos gran parte de la razón por la que se creó una Intranet en primer lugar es que la Web facilita la publicación de la información y formularios por toda la compañía usando el Lenguaje de Marcado de Hipertexto (HTML). La Web permite la creación de páginas iniciales multimedia, que están compuestos de texto, gráficos, y contenidos multimedia como sonido y vídeo. Los enlaces de hipertexto te permiten saltar desde un lugar en la Web a otro, lo que significa que puedes saltar a lugares dentro de una Intranet o fuera en Internet desde una pagina inicial.

Las Intranets están basadas en la arquitectura cliente / servidor. EL software cliente-un navegador para Web, se ejecuta en una computadora local, y el software servidor en una Intranet anfitriona. El software cliente esta disponible para PC, Macintosh y estaciones de trabajo UNÍS. El software servidor se ejecuta en UNÍS, Windows NT y otros sistemas operativos. El software cliente y el software servidor no necesitan ejecutarse en el mismo sistema operativo. Para una Intranet, primero pone en marcha tu navegador para Web. Si estás conectado directamente con tu Intranet, el programa TCP/IP que necesitas para ejecutar el navegador ya estará instalado en tu computadora.

Cuando se ponen en marcha los navegadores, visitarán una cierta localización predeterminada. En una Intranet, esa localización puede ser una

página Web departamental o una página Web por toda la compañía. Para visitar un sitio diferente, escribe la localización de la Intranet que quieres visitar, o pulsa en un enlace para dirigirte allí. El nombre para cualquier localización Web es el URL(localizador uniforme de recursos). Tu navegador para Web envía la petición URL usando http(Protocolo de Transferencia de Hipertexto) que define el modo en el que se comunican el navegador para Web y el servidor Web.

Si la petición es de una página localizada en la Intranet, los navegadores envían la petición a esa página Web de la Intranet. Puede estar disponible una conexión de alta velocidad, puesto que las Intranet pueden construirse usando cables de alta velocidad, y todo el tráfico dentro de la Intranet se puede conducir por esos cables. La conexión Internet puede ser mucho más lenta debido a la cantidad de tráfico de Internet, y porque puede haber varias conexiones de baja velocidad que la petición desde la Intranet tendrá que atravesar. Los paquetes que componen la petición se encaminan hacia un enrutador de la Intranet, que envía en turnos la petición al servidor Web.

El servidor Web recibe la petición usando http, la petición es para un documento específico. Devuelve la página inicial, documento u objetivo al navegador para Web cliente. La información se muestra ahora en la pantalla de la computadora en el navegador Web. Después de enviar el objeto al navegador para Web, la conexión http se cierra para hacer un uso más eficaz de los recursos de la red.

Los URL constan de varia partes. La primera parte, el http://, detalla qué protocolo Internet hay que usar. El segmento www.zdnet.com" varia en longitud e identifica el servidor Web con el que hay que contactar. La parte final

identifica un directorio específico en el servidor, y una página inicial, documento, u otro objeto de Internet o de la Intranet.

**COMO FUNCIONAN LOS SERVIDORES DE SISTEMAS DE NOMBRES DE DOMINIO EN LAS INTRANETS**

Cuando hay que conectar con un URL particular, la dirección con el URL debe ser igual que la dirección IP verdadera. Tu navegador para Web irá primero a un servidor DNS local en la Intranet de la empresa para obtener esta información si la dirección IP es local, el servidor DNS podrá resolver el URL con la dirección IP. Este enviará la dirección IP auténtica a tu computadora.

Tu navegador para Web tiene ahora la dirección IP verdadera del lugar que estás intentando localizar. Utiliza esa dirección IP y contacta con el sitio. EL sitio te envía la información que has solicitado.

Si la información que has solicitado no está en tu Intranet, y si tu servidor DBS local no tiene la dirección IP, el servidor DNS de Intranets debe obtener la información desde un servidor DNS en Internet. EL servidor DNS de Intranets contacta con lo que se denomina servidor de dominio raía, que se mantiene por un grupo llamado InterNiC. EL servidor raíz e dominio l dice al servidor de Intranets qué servidor primario de nombres y qué servidor secundario de nombres tiene la información sobre el URL solicitado.

El servidor de Intranets contacta ahora con el servidor primario de nombres. Si la información no se puede encontrar en el servidor primario de nombres, el servidor DNS de Intranets contacta con el servidor secundario. Uno de esos servidores de nombres tendrá la información exacta. Después devolverá la información al servidor DNS de Intranets.

El servidor DNS de Intranets te devuelve la información, tu navegador para Web usa ahora la dirección IP para contactar con el sitio exacto.

Cuando alguien en una Intranet quiere contactar con una localización, por ejemplo, visitar un sitio Web, escribirá una dirección, como www.metahouse.com. Aunque de hecho, Internet no utiliza realmente estas direcciones alfanuméricas. En lugar de eso, emplea direcciones IP, que son direcciones numéricas, en cuatro números de 8 bits separados por puntos, como 123.5.56.255. Un servidor DNS, llamado también un servidor de nombres, empareja, direcciones alfanuméricas con sus direcciones IP, y te permite contactar con la localización exacta.

**SUBDIVIDIR UNA INTRANET**

Cuando las Intranets sobrepasan un cierto tamaño, o se extienden por varias localizaciones geográficas, empiezan a ser difícil manejarlas como una sola red. Para resolver el problema, la Intranet se puede subdividir en varias subredes, sub-secciones de una Intranet que las hacen más fáciles de administrar. Para el mundo exterior, la Intranet aparece todavía como su fuera una sola red.

Si estas construyendo una Intranet y quieres que este conectada con Internet, necesitarías una dirección IP única para tu red, que será manejada por los Servicios Internic de Registro. Puedes disponer de tres clases de redes: Clase A, Clase B o Clase C. Generalmente, la clasificación de Clase A es mejor para las redes más grandes, mientras que la Clase C es mejor para las más pequeñas. Una red de Clase A puede estar compuesta de 127 redes y un total de 16.777.214 nodos en la red. Una red de Clase B puede estar compuesta de

16.383 redes y un total de 65.383 nodos. Una red de Clase C puede estar compuesta de 2.097.151 redes y 254 nodos.

Cuando se le asigna una dirección a una Intranet, se asigna los dos primeros números IP de la dirección Internet numérica (llamados el campo de la net-id) y los dos números restantes (llamados el campo de la host-id) se dejan en blanco, para que la propia Intranet los pueda asignar, como 147.106.0.0. El campo de la host-id consiste en un número para una subred y un número de anfitrión.

Cuando una Intranet se conecta con Internet, un enrutador realiza el trabajo de enviar los paquetes desde Internet a la Intranet.

Cuando las Intranets crecen, por ejemplo, si hay un departamento ubicado en otro edificio, ciudad o país, se necesita algún método para manejar el tráfico de red. Puede ser poco práctico y físicamente imposible encaminar todos los datos necesarios entre muchas computadoras diferentes extendidos por un edificio o por el mundo. Se necesita crear una segunda red denominada subred de trabajo o subred.

Para tener un enrutador que dirija todo él trafico de entrada para un Intranet subdividida, se utiliza el primer byte del campo de la host-id. Los bits que se usan para distinguir subredes se llaman números de subred.

Cada computadora en cada subred recibe su propia dirección IP, como en una Intranet normal. La combinación del campo de la net-id el número de subred, y finalmente un número de anfitrión, forman la dirección IP.

El enrutador debe ir informado de que el campo de la host-id en las subredes tiene que tratarse de modo diferente que los campos del a host-id no subdivididos, si no en así, no podrá encaminar adecuadamente los datos. Para

hacer esto, se emplea una mascara de subred. Una mascara de Subred es un número de 32 bits como 255.255.0.0, que se utiliza conjuntamente con los números en el campo dela host-id. Cuando se efectúa un calculo usando la mascara de subred y la dirección IP, el enrutador sabe donde encamina el correo. La mascara de subred está incluida en los archivos de configuración de la red de los usuarios.

**COMO FUNCIONA LA CONVERSIÓN DE REDES IPX EN UNA INTRANET**

La mayoría de las Intranets no están construidas desde cero. Muchas son redes existentes, como Novell NetWare, que tienen que convertirse en una Intranet. A menudo, el primer paso en el movimiento hacia una Intranet puede introducirse en la propia red existente. Depuse, la tecnología de Intranets puede introducirse en la propia red y convertirse en una Intranet.

Cuando una computadora en la red quiere conectar con Internet y solicitar información de ella, se envía una petición a un navegador en la Intranet. Este navegador enviará la petición al destino exacto en Internet. En la red NetWare, el sistema operativo NetWare se utiliza para manejar el tráfico de la red y la administración. Como método para encaminar paquetes a través de la red, NetWare emplea al protocolo IPX (Intercambio de Paquetes Internet). Aunque IPX se denomina intercambio de paquetes Internet, no ofrece realmente acceso a Internet o transporta la información de Internet. Las estaciones de trabajo pertenecientes a la red NetWare, y los servidores en la red, necesitan tener cargado IPX en la memoria para usar la red.

Para que las estaciones de trabajo en la red Novell consiga acceder a Internet o a la Intranet, necesitan ejecutar los protocolos TCP/IP que forman la base de Internet. Para hacer eso, debe instalarse una pila TCP/IP en cada computadora que permitirá la entrada a la Intranet. Esto significa que cada computadora tendrá instalado IPX y una pila TCP/IP, para permitir el acceso a Internet y a la red Ethernet. Básicamente, esto da como resultado "RAM de bote en bote" y es uno de los dolores de cabeza más fuertes para cualquiera que intente ejecutar ambas pilas de protocolos. Una unidad de servicio de canal/Unidad de Servicio de Datos (CSU/DSU) realiza la conexión física entre el enrutador de la Intranet y el Proveedor de Servicio Internet (IPS). EL ISP ofrece la autentica conexión Internet y servicios. Varias líneas digitales pueden conectar la CSU/DSU con el ISP, incluyendo una línea alquilada de 56 Kbps, una línea T1 de alta velocidad, o incluso una líneat3 de mayor velocidad. La información solicitada se devuelve a través del CSU/DSU y del enrutador, y después se encamina a la computadora que pidió la información. Si la información está ubicada en una Intranet dentro de la compañía, el enrutador enviará la petición al anfitrión exacto, que después devolverá la información al solicitante. Algunos productos como NetWare/IP permitirán a las computadoras acceder a servicios de NetWare y a Internet. Esto significa que no tienen que ejecutar los protocolos IPX y TCP/IP, eliminando los problemas de memoria producidos por las múltiples pilas.

**SEGURIDAD DE LAS INTRANETS**

Cualquier Intranet es vulnerable a los ataques de personas que tengan el propósito de destruir o robar datos empresariales. La naturaleza sin límites

de Internet y los protocolos TCP/IP exponen a una empresa a este tipo de ataques. Las Intranets requieren varias medidas de seguridad, incluyendo las combinaciones de hardware y software que proporcionan el control del tráfico; la encriptación y las contraseñas para convalidar usuarios; y las herramientas del software para evitar y curar de virus, bloquear sitios indeseables, y controlar el tráfico.

El término genérico usado para denominar a una línea de defensa contra intrusos es firewall. Un firewall es una combinación de hardware / software que controla el tipo de servicios permitidos hacia o desde la Intranet.

Los servidores sustitutos son otra herramienta común utilizada para construir un firewall. Un servidor sustituto permite a los administradores de sistemas seguir la pista de todo el tráfico que entra y sale de una Intranet.

Un firewall de un servidor bastión se configura para oponerse y evitar el acceso a los servicios no autorizados. Normalmente está aislado del resto de la Intranet en su propia subred de perímetro. De este modo si el servidor es "allanado", el resto de la Intranet no estará en peligro. Los sistemas de autenticación son una parte importante en el diseño de la seguridad de cualquier Intranet. Los sistemas de autenticación se emplean para asegurar que cualquiera de sus recursos, es la persona que dice ser. Los sistemas de autenticación normalmente utilizan nombres de usuario, contraseñas y sistemas de encriptación.

El software para el bloqueo de sitios basado en el servidor de sitios basado en el servidor puede prohibir a los usuarios de una Intranet la obtención de material indeseable. EL software de control rastrea dónde ha ido la gente y qué servicios han usado, como HTTP para el acceso a la Web. El software

para detectar virus basado en el servidor puede comprobar cualquier archivo que entra en la Intranet para asegurarse que está libre de virus.

Una manera de asegurarse de que las personas impropias o los datos erróneos no pueden acceder a la Intranet es usar un enrutador para filtrar. Este es un tipo especial de enrutador que examina la dirección IP y la información de cabecera de cada paquete que entra en la Intranet, y sólo permite el acceso a aquellos paquetes que tengan direcciones u otros datos, como e-mail, que el administrador del sistema ha decidido previamente que pueden acceder a la Intranet.

## COMO FUNCIONAN LOS ENRUTADORES PARA FILTRAR

Los enrutadores para filtrar, algunas veces denominados enrutadores de selección, son la primera línea de defensa contra ataques a la Intranet. Los enrutadores para filtrar examinan cada paquete que se mueve entre redes en una Intranet. Un administrador de Intranets establece las reglas que utilizan los enrutadores para tomar decisiones sobre qué paquetes debería admitir o denegar.

Las distintas reglas se pueden establecer para paquetes que entran y que salen de modo que los usuarios de Intranets puedan acceder a los servicios de Internet, mientras que cualquiera en Internet tendría prohibido el acceso a ciertos servicios y datos de la Intranet. Los enrutadores para filtrar pueden llevar el registro sobre la actividad de filtración. Comúnmente, siguen la pista a los paquetes sin permiso para pasar entre Internet y la Intranet, que indicarían que una Intranet ha estado expuesta al ataque.

Las direcciones de origen se leen desde la cabecera IP y se comparan con la lista de direcciones de origen en las tablas de filtros. Ciertas direcciones pueden ser conocidas por ser peligrosas y al incluir en la tabla permiten el enrutador denegar ese tráfico. El enrutador examina los datos en la cabecera IP que envuelve los datos y la información de cabecera de la pila de transporte. Eso significa que cualquier paquete contendrá datos, y dos conjuntos de cabeceras: una para la pila de transporte y otra para la pila de Internet. Los enrutadores para filtrar examinan todos estos datos y cabecera para decidir si permiten pasar a los paquetes. Los enrutadores pueden tener reglas diferentes para las sub - redes ya que pueden necesitar distintos niveles de seguridad. Una subred que contenga información privada financiera o competitiva puede tener muchas restricciones. Una subred de ingeniería puede tener menos restricciones en actividad que entran o salen.

Un enrutador para filtrar puede permitir a los usuarios tener acceso a servicios como Telnet y FTP, mientras que restringe el uso de Internet de estos servicios para acceder a la Intranet. Esta misma técnica se puede emplear para evitar que los usuarios internos accedan a datos restringidos de una Intranet. Por ejemplo, puede permitir a los miembros financieros el uso abierto de FTP mientras que deniega las peticiones FTP del departamento de ingeniería en el departamento de finanzas. Cierto tipo de servicios son más peligrosos que otros. Por ejemplo, FTP se utiliza para recibir archivos pero puede traer archivos que contengan un virus. Telnet y el comando roglin (que es como Telnet pero con mayor riesgo de burlar la seguridad) están prohibidos por las reglas en la tabla de filtros que evalúan este tipo de servicio por él numero del puerto de origen o destino. Trucar direcciones es un método de ataque común.

Para trucar direcciones, alguien externo a la Intranet falsifica una dirección de origen de modo que el enrutador le parezca que la dirección de origen es realmente de alguien de dentro de la Intranet. El bromista espera engañar al enrutador para filtrar para que le permita un mayor acceso a la Intranet que el que le permite una dirección externa original. Una vez que el enrutador se convenció de que el bromista estaba ya dentro de la Intranet, los archivos privados podrían enviarse potencialmente fuera de la Intranet. Los enrutadores pueden manejar direcciones truncadas. Se puede establecer una regla que comunique al enrutador examinar la dirección de origen en cada cabecera IP que entre, pero que no salga. Si la dirección de origen es interna, pero el paquete proviene del exterior, el enrutador no admitirá el paquete.

**COMO FUNCIONAN LOS FIREWALLS**

Los firewalls protegen a las Intranets de los ataques iniciados contra ellas desde Internet. Están diseñados para proteger a una Intranet del acceso no autorizado a la información de la empresa, y del daño o rechazo de los recursos y servicios informáticos. También están diseñados para impedir que los usuarios internos accedan a los servicios de Internet que puedan ser peligrosos, como FTP.

Las computadoras de las Intranets sólo tienen permiso para acceder a Internet después de atravesar un firewall. Las peticiones tienen que atravesar un enrutador interno de selección, llamado también enrutador interno para filtrar o enrutador de obstrucción. Este enrutador evita que el trafico de paquetes sea "husmeado" remotamente. Un enrutador de obstrucción examina la información de todos los paquetes como cuál es su origen y cuál su destino. El enrutador

compara la información que encuentra con las reglas en una tabla de filtros, y admite, o no, los paquetes basándose en esas reglas. Por ejemplo, algunos servicios, como login, no pueden tener permiso para ejecutarse. El enrutador no permite tampoco que cualquier paquete se envíe a localizaciones específicas del Internet sospechosas. Un enrutador también puede bloquear cada paquete que viaje entre Internet y la Intranet, excepto el e-mail. Los administradores de sistemas qué paquetes admitir y cuáles denegar. Cuando una Intranet está protegida por un firewall, están disponibles los servicios internos usuales de la red, como el e-mail, el acceso a las bases de datos corporativas y a los servicios de la Web, y el uso de programas para el trabajo en grupo.

Los firewall seleccionados de la subred tiene una manera más para proteger la Intranet: un enrutador exterior de selección, también denominado enrutador de acceso. Este enrutador selecciona paquetes entre Internet y la red de perímetro utilizando el mismo tipo de tecnología que el enrutador interior de selección. Puede seleccionar paquetes basándose en las mismas reglas que plica el enrutador interior de selección y puede proteger a la red incluso si el enrutador interno falla. Sin embargo, también puede tener reglas adicionales para la selección de paquetes diseñadas eficazmente para proteger al anfitrión bastión. Como un modo adicional para proteger a una Intranet del ataque, el anfitrión bastión se coloca en una red de perímetro, una subred, dentro del firewall. Si el anfitrión bastión estuviera en la Intranet en vez de en una red de perímetro y fuera, el intruso podría obtener acceso a la Intranet. Un anfitrión bastión es el punto de contacto principal para las conexiones provenientes de Internet para todos los servicios como el e-mail, el acceso FTP, y cualquier

otros datos y peticiones. El anfitrión bastión atiende todas esas peticiones, las personas en la Intranet sólo se ponen en contacto con este servidor, y no contactan directamente con otros servidores de Intranets. De este modo, los servidores de Intranets están protegidos del ataque. Los anfitriones bastión también pueden configurarse como servidores sustitutos.

## COMO FUNCIONAN LOS SERVIDORES SUSTITUTOS

Una parte integral de muchos de los sistemas de seguridad es el servidor sustituto. Un servidor sustituto software y un servidor que se coloca en un firewall y actúa como intermediario entre computadoras en una Intranet e Internet. Los servidores sustitutos a menudo se ejecutan en anfitriones bastón. Solo el servidor sustituto en vez de las muchas computadoras individuales en la Intranet, interactúan con Internet, de este modo la seguridad se puede mantener porque el servidor puede estar más seguro que los cientos de computadoras individuales en la Intranet. Los administradores de Intranets pueden configurar servidores sustitutos que puedan utilizarse para muchos servicios, como FTP, la Web y Telnet. Los administradores de Intranets deciden que servicios de Internet deben atravesar un servidor sustituto, y cuales no. Se necesita software especifico del servidor sustituto para cada tipo diferente de servicio Internet.

Cuando una computadora en la Intranet realiza una petición a Internet, como recuperar una página Web desde un servidor Web, la computadora interna se pone en contacto con el servidor Internet, El servidor Internet envía la página Web al servidor sustituto, que después la mandará a la computadora de la Intranet. Los servidores sustitutos registran todo en tráfico entre Internet y

la Intranet, por ejemplo, un servidor sustituto de Telnet podría seguir la pista de cada pulsación de una tecla en cada sección Telnet en la Intranet, y también podría seguir la pista de cómo reacciona al servidor externo en Internet con esas pulsaciones. Los servidores sustitutos pueden anotar cada dirección IP, fecha y hora de acceso, URL, número de bytes recibidos, etc. Esta información se puede utilizar para analizar cualquier ataque iniciado contra la red. También puede ayudar a los administradores de Intranets a construir mejor acceso y servicios para los empleados. Algunos servidores sustitutos tienen que trabajar con clientes sustitutos especiales. Una tendencia más popular es usar clientes con servidores sustitutos ya configurados como Netscape. Cuando se emplea este paquete ya hecho, debe configurarse especialmente para trabajar con servidores sustitutos desde el menú de configuración. Después el empleado de la Intranet usa el software cliente como de costumbre. El software cliente sabe salir hacia un servidor sustituto para obtener datos, en vez de hacia Internet.

Los servidores sustitutos pueden hacer algo más que hacer llegar las peticiones entre una Intranet e Internet. También pueden hacer efectivos los diseños de seguridad. Por ejemplo podría configurarse para permitir en envío de archivos desde Internet a una computadora de la Intranet, pero impedir que se manden archivos desde la red empresarial a Internet, o viceversa. De este modo, los administradores de Intranets pueden impedir que cualquier persona externa a la corporación reciba datos corporativos vitales. O pueden evitar que los usuarios de la Intranet reciban archivos que puedan contener virus. Los servidores sustitutos también se pueden utilizar para acelerar la actuación de algunos servicios de Internet almacenando datos. Por ejemplo, un servidor Web sustituto podría almacenar muchas paginas Web, a fin de que cuando

alguien desde la Intranet quisiera obtener alguna de esas páginas Web, accediera ella directamente desde el servidor sustituto a través de líneas de la Intranet de alta velocidad, en lugar de tener que salir a través de Internet y obtener la página a menor velocidad desde las líneas de Internet.

## COMO FUNCIONAN LOS ANFITRIONES BASTIÓN

Un anfitrión bastión (llamado también servidor bastón) es una de las defensas principales en el firewall de una Intranet. Es un servidor fuertemente fortificado que se coloca dentro del firewall, y es el punto de contacto principal de la Intranet e Internet. Al tener como punto de contacto principal un servidor aislado, duramente defendido, el resto de los recursos de la Intranet pueden proteger de los ataques que se inician en Internet.

Los anfitriones bastión se construyen para que cada servicio posible de la red quede inutilizado una vez dentro de ellos, lo único que hace el servidor es permitir el acceso especifico de Internet. Así que, por ejemplo, no debería haber ninguna cuenta de usuarios en n servidor bastión, para que nadie pudiera entrar, tomar el control y después obtener acceso a la Internet. Incluso el Sistema de Archivos de Red (NFS), que permite a un sistema el acceso a archivos a través de una red en un sistema remoto, debería inhabilitarse para que los intrusos no pudieran acceder al servidor bastión es instalarlo en su propia subred como parte del firewall de una Intranet. Al colocarlos en su propia red, si son atacados, ningún recurso de la Intranet se pone en peligro.

Los servidores bastión registran todas las actividades para que los administradores de Intranets puedan decir la red ha sido atacada. A menudo guardan dos copias de los registros del sistema por razones de seguridad: en

caso de que se destruya o falsifique un registro, el otro siempre disponible como reserva. Un modo de guardar una copia segura del registro es conectar el servidor bastión mediante un puerto de serie con una computadora especializada, cuyo único propósito es seguir la pista del registro de reserva.

Los monitores automatizados son programas incluso más sofisticados que el software de auditoria. Comprueban con regularidad los registros del sistema del servidor bastión, y envían una alarma si encuentra un patrón sospechoso. Por ejemplo, se puede enviar una alarma si alguien intenta más de tres conexiones no exitosas. Algunos servidores bastión incluyen programas de auditoria, que examinan activamente si se ha iniciado un ataque en su contra. Hay varias maneras de hacer una auditoria: una manera de revisar esto es utilizar un programa de control que compruebe si algún software en el servidor bastión se ha modificado por una persona no autorizada. El programa de control calcula un número basándose en el tamaño de un programa ejecutable que hay en el servidor. Después calcula con regularidad el número de control para ver si ha cambiado desde la última vez que lo hizo. Si ha cambiado, significa que alguien ha alterado el software, lo que podría indicar un ataque externo.

Cuando un servidor bastión recibe una petición de un servidor como puede ser enviar una pagina Web o repartir e-mail, el servidor no administra la petición él mismo; en su lugar, envía la petición al servidor de Intranets apropiado. EL servidor de Intranets maneja la petición, y después devuelve la información al servidor bastión; y será ahora cuando envíe la información requerida al solicitarme en Internet.

Puede haber más de un anfitrión bastión en un firewall; y cada uno puede administrar varios servicios de Internet para la Intranet. Algunas veces, un anfitrión bastión se puede utilizar como maquina victima: un servidor despojado de casi todos los servicios excepto de uno especifico de Internet. Las máquinas victimas pueden emplearse para ofrecer servicios de Internet que son difíciles de manejar o cuyas limitaciones sobre la seguridad no se conocen aún, utilizando un enrutador sustituto o uno para filtrar. Los servidores se colocan en la máquina victima en vez de en un anfitrión bastión con otros servicios. De ese modo, si se irrumpe en el servidor, los otros anfitriones bastión no estarán afectados.

**COMO FUNCIONA LA ENCRIPTACIÓN**

Un medio de asegurar una Intranet es usar la encriptación: alterar datos para que sólo alguien con acceso a códigos específicos para descifrar pueda comprender la información. La encriptación se utiliza para almacenar y enviar contraseña para asegurarse de que ningún fisgón pueda entenderla. La encriptación se emplea también cuando se envían datos entre Intranets en Redes Privadas Muy Seguras (VSPN). Además la encriptación se usa para dirigir el comercio en Internet y proteger la información de la tarjeta de crédito durante la transmisión.

Las claves son el centro de la encriptación. Las claves son formulas matemáticas complejas (algoritmos), que se utilizan para cifrar y descifrar mensajes. Si alguien cifra un mensaje sólo otra persona con la clave exacta será capaz de descifrarlo. Hay dos sistemas de claves básicos: criptografía de claves secretas y de claves públicas. Se emplea un algoritmo para realizar una

función de rehecho. Este proceso produce un resumen del mensaje único al mensaje. El resumen del mensaje se cifra con la clave privada del emisor que da lugar a una "huella digital".

El estándar de Encriptación de Datos (DES) es un sistema de claves secretas (simétrico); no hay componente de clave privada. El emisor y el receptor conocen la palabra secreta del código. Este método no es factible para dirigir negocios por Internet. RSA es un sistema de claves públicas (asimétrico), que utiliza pares de claves para cifrar y descifrar mensajes. Cada persona tiene una clave pública, disponible para cualquiera en un anillo de claves públicas, y una clave privada, guardada sólo en la computadora. Los datos cifrados con la clave privada de alguien sólo pueden descifrarse con su clave pública, y los datos cifrados con su clave pública sólo pueden descifrarse con su clave privada. Por tanto, RSA necesita un intercambio de claves públicas, esto se puede realizar sin necesidad de secretos ya que la clave pública es inútil sin la clave privada.

PGP, Privacidad de las buenas, un programa inventado por Philip Zimmermann, es un método popular empleado para cifrar datos. Utiliza MD5 (resumen del mensaje 5) y los sistemas cifrados de RSA para generar los pares de claves. Es un programa muy extendido que se puede ejecutar en plataformas UNÍX, DOS y Macintosh. Ofrece algunas variaciones de funcionalidad, como la comprensión, que otros sistemas cifrados no brindan. Los pares de claves múltiples se pueden generar y ubicar en anillos de claves públicas y privadas.

**COMO FUNCIONAN LAS CONTRASEÑAS Y LOS SISTEMAS DE AUTENTICACION**

Una de las primeras líneas de defensa de una Intranet es usar la protección de las contraseñas. Varias técnicas de seguridad, incluyendo la encriptación, ayudan a asegurarse de que las contraseñas se mantienen a salvo. También es necesario exigir que las contraseñas se cambien frecuentemente, que no sean adivinadas fácilmente o palabras comunes del diccionario, y que no se revelen simplemente. La autenticación es el paso adicional para verificar que la persona que ofrece la contraseña es la persona autorizada para hacerlo.

El servidor cifra la contraseña que recibe del usuario, utilizando la misma técnica de encriptación empleada para cifrar la tabla de contraseñas del servidor. Compara la contraseña cifrada del usuario con la contraseña cifrada en la tabla. Si los resultados encajan, el usuario tiene permiso para entrar en el sistema. Si los resultados no encajan, el usuario no tiene permiso.

Las contraseñas de la gente y los nombres de usuario en una Intranet se almacena dentro de un formulario de tablas de un archivo que se encuentra en un servidor que verifica las contraseñas. A menudo, el nombre del archivo es password y el directorio en el que se encuentra es etc. Dependiendo de la técnica de autenticación de contraseñas que se use, el archivo puede estar cifrado o no.

Un método para reconocer a un usuario es a través del Protocolo de Autenticación de Contraseñas (PAP). PAP no asigna la encriptación, pero la tabla de contraseñas en el servidor está normalmente cifrada. Cuando alguien

quiere entrar a la red o a un recurso de la red protegido con una contraseña, se le pide el nombre de usuario y la contraseña. El nombre de usuario y la contraseña se envía después al servidor.

El sistema del Protocolo de Autenticación para Cuestionar el Handshake (CHAP) es un sistema de respuesta. El CHAP requiere una tabla de contraseñas no cifrada. Cuando alguien entra en un sistema con CHAP, el servidor genera una clave al azar que se envía al usuario para que cifre su contraseña.

La computadora del usuario emplea esta clave para cifrar su contraseña. Después la contraseña cifrada se devuelve al servidor. El servidor se remite a la tabla de contraseñas para la clave al azar, y cifra la contraseña con la misma clave que se envió al usuario. El servidor compara después la contraseña cifrada con la del usuario con la contraseña cifrada que creó. Si encajan, el usuario tiene permiso de entrada.

La clave de diferencia de CHAP en que el servidor continúa preguntando a la computadora del usuario a lo largo de la sesión. Además, se envía distintas preguntas que deben ser cifradas y devueltas por la computadora, sin intervención humana. De este modo CHAP limita tu ventana de vulnerabilidad. Una sesión no puede piratearse, puesto que el pirata no sería admitido una vez que la computadora no respondiera correctamente a los desafíos que se suceden periódicamente.

Sin importar qué tipo de sistemas de contraseñas se utilice, ni la tabla de contraseñas está cifrada o no, lo importante es proteger la tabla de contraseñas. El archivo debe protegerse contra el acceso FTP y debería haber

acceso restringido al archivo para que sólo el administrador o alguien bajo el control del administrador puedan acceder a él.

**COMO FUNCIONA EL SOFTWARE PARA EXAMINAR VIRUS EN UNA INTRANET**

Los virus son el mayor riesgo en la seguridad de las Intranets. Pueden dañar datos, ocupar y consumir recursos, e interrumpir operaciones. Los archivos de programas eran la principal fuente de problemas en el pasado, pero los nuevos virus de "macro" se pueden esconder en archivos de datos e iniciarse, por ejemplo, cuando se ejecutan una macro en un programa de procesamiento de texto. El software para examinar virus basado en el servidor y el basado en el cliente poseen dispositivos que ayudan a proteger a la Intranet.

Un virus se esconde dentro de un programa. Hasta que ejecutes el programa infectado, el virus permanece inactivo, entonces el virus entra en acción. Algunas veces, lo primero que se hará infectar otros programas del disco duro copiándose de ellos.

Algunos virus colocan mensajes denominados V-marcadores o marcadores de virus dentro de programas que están infectados y ayudan a manejar las actividades víricas. Cada virus tiene un marcador de virus especifico asociado con él. Si un virus se encuentra con uno de estos marcadores en otro programa, sabe que el programa ya está infectado y de ese modo no se reproduce allí. Cuando un virus no encuentra ningún archivo sin marcar en una computadora, eso puede indicar al virus que no hay que infectar más archivos. En este momento, el virus empieza a estropear la computadora y

sus datos. Los virus no pueden corromper los archivos de programas o de datos ya que cuando se ejecutan funcionan extrañamente, no funcionan o causan daños. Pueden destruir todos los archivos de tu computadora necesita cuando se conecta y provocar otro tipo de averías.

El software para examinar virus se ejecuta en un servidor dentro del firewall de una Intranet. El software no comprueba la posible existencia de virus en cada paquete que entra en la Intranet, ya que eso sería imposible. En su lugar, sólo comprueba aquellos paquetes enviados con los tipos de servicios y protocolos Internet que indican que un archivo puede encontrarse en el proceso de transferencia desde Internet, comúnmente, e-mail (que se envía mediante SMTP, (Protocolo Simple de Transferencia de Correo), el Protocolo de Transferencia de Archivos (FTP) y la World Wide Web (http; Protocolo Transferencia de Hipertexto). EL software emplea la tecnología de filtrado de paquetes para determinar qué paquetes se están enviando con estos protocolos.

Cuando el software encuentra paquetes que se envían con SMTP, FTP o HTTP, sabe que debe examinarlos más a fondo, para ver si tienen virus. El software para examinar virus funciona de varias maneras. Un método de detección es comprobar archivos para revelar marcadores de virus que indican la presencia de un virus. Los paquetes que no están utilizando SMTP, FTP o http (como TNP) se admiten y el software no realiza ninguna acción en ellos.

Si se encuentra que el archivo está libre de virus, se le permite pasar. Si se encuentra que tiene virus, no se le permitirá entrar en la Intranet.

El software antivirus también debería ejecutarse en computadoras individuales dentro de la Intranet porque es posible que se pueda introducir un

virus en la Intranet por disquetes, por ejemplo. Además de la protección contra virus, puede detectar virus y extirpar cualquier virus que encuentre.

## BLOQUEAR SITIOS INDESEABLES DESDE UNA INTRANET

El software para el bloqueo de sitios examina el URL de cada petición que sale de la Intranet. Los URL más propensos a no ser aceptados accederán a la Web (http); grupos de noticias (ntp), ftp (ftp); gopher (gopher) y las conversaciones de Internet (irc). EL software toma cada uno de estos cinco tipos de URL y los pone en sus propias "cajas" separadas. El resto de la información de la Intranet que sale tiene permiso para pasar.

Cada URL en cada caja se comprueba en una base de datos de los URL de los sitios censurables. Si el software de bloqueo encuentra que algunos de los URL provienen de sitios desagradables, no permitirá que la información pase a la Intranet. Los productos como SurfWatch como prueban miles de sitios y enumeran varios miles en sus bases de datos que se han encontrado molestos.

El software para bloquear sitios comprueba después el URL con una base de datos de palabras (como "sexo") que puede indicar que el material que se solicita puede ser censurable. Si el software de bloqueo encuentra un patrón que encaje, no permitirá que la información pase a la Intranet.

El software para bloquear sitios puede entonces emplear un tercer método para comprobar los sitios desagradables; un sistema de clasificación llamado PICS (Plataforma para la Selección de Contenido en Internet). Si el software para el bloqueo de sitios encuentra, basándose en el sistema de

clasificación, que el URL es para un sitio que puede contener material censurable, no permitirá el acceso a ese sitio.

Debido a que Internet está creciendo tan deprisa, las bases de datos de sitios censurables podrían llegar a ser anticuados. Para resolver el problema, la base de datos se actualiza cada mes. El software para el bloqueo de sitios conectará automáticamente con un sitio en Internet, y recibirá la base de datos de sitios desagradables más nueva a través de ftp.

Los administradores de Intranets pueden encontrar sitios no enumerados en la base de datos y no filtrados por el software para bloquear sitios que ellos quieren bloquear. Para bloquear manualmente el acceso a esos sitios, pueden añadirlos simplemente a la base de datos.

**COMO FUNCIONA EL SOFTWARE DE SUPERVISIÓN DE INTRANETS**

El software utiliza filtrado de paquetes, muy parecidos a lo que hacen los enrutadores para filtrar. Ambos observan los datos en la cabecera de cada paquete IP que entra y sale de la Intranet. Sin embargo, se diferencian en que los enrutadores para filtrar deciden si admiten o no a los paquetes. El software de supervisión simplemente deja pasar a los paquetes y sigue la pista a la información de los paquetes además delos datos como la dirección del emisor y destino, el tamaño del paquete, el tipo de servicio de Internet implicado (como la WEB o FTP) y la hora del día en la que se recogen en una base de datos.

Mientras que todos los paquetes deben pasar a través del servidor, el software no introduce necesariamente la información de cada paquete en la base de datos. Por ejemplo, la información acerca de los paquetes http (World

Wide Web), los paquetes del protocolo de transferencia de archivos (FTP), los paquetes del protocolo de transferencia de archivos (FTP), los paquetes e-mail (SMTP), los paquetes delos grupos de noticias (TNP) y los paquetes Telnet pueden seguirse, mientras que los paquetes de sonido fluido pueden ignorarse.

El software incluido con el programa del servidor permite a los administradores de redes examinar y analizar el tráfico de la Intranet y de Internet en un grado extraordinario. Puede mostrar la cantidad total del tráfico de la red por día y por horas, por ejemplo, y mostrar a cualquier hora a qué sitios de Internet se estaban transfiriendo. Puede incluso mostrar qué sitios estaban visitando los usuarios individuales en la Intranet, y los sitios más populares visitados en forma gráfica.

Algún software va más allá del análisis y permite a los administradores de Intranets cambiar el tipo de acceso a Internet de los usuarios de la Intranet, basándose en el tráfico, uso y otros factores. El software permitirá también a los administradores de Intranets prohibir que se visiten ciertos sitios de la Intranet.

## COMO FUNCIONAN LAS HERRAMIENTAS DE BÚSQUEDA DE LAS INTRANETS

Las herramientas de búsqueda y de catalogación, como agentes, arañas, tractores y autómatas, algunas veces denominadas motores de búsqueda, se pueden utilizar para ayudar a la gente a encontrar información y se emplean para reunir información acerca de documento disponibles en una Intranet. Estas herramientas de búsqueda son programas que buscan paginas Web, obtienen los enlaces de hipertexto en esas paginas y clasifican la

información que encuentran para construir una base de datos. Cada moto de búsqueda tiene su propio conjunto de reglas. Algunos siguen cada enlace en todas las paginas que encuentran, y después en turno examinan cada enlace en cada una de esas paginas iniciales nuevas, etc. Algunos ignoran enlaces que dirigen a archivos gráficos, archivos de sonido y archivos de animación; algunos enlaces a ciertos recursos como las bases de datos WAIS; y a algunos se les dan instrucciones para buscar las páginas iniciales más visitadas.

**COMO FUNCIONAN LAS TRANSACIONES FINANCIERAS EN UNA INTRANET**

Las Intranet se utilizan no sólo para coordinar negocios y hacerlos más eficaces, sino también como un lugar para hacerlos - recibir y rellenar pedidos de bienes y servicios. Aunque para que esto ocurra, se debe diseñar una manera segura para enviar la información de la tarjeta de crédito por la notoriamente insegura Internet. Hay muchos métodos para hacer esto pero probablemente el que más se utilizará será un estándar llamado: el protocolo para la Transacción Electrónica Segura (SET), que ha sido aprobado por VISA, MasterCard, American Express, Microsoft y Nestcape, entre otras compañías. Es un sistema que permitirá a la gente con tarjetas bancarias hacer negocios seguros por las Intranets.

**CONCLUSION**

Con la evolución que cada día sufre los sistemas de computación, su fácil manejo e innumerables funciones que nos ofrece, su puede decir que igualmente se ha incrementado el numero de usuarios que trabajan con

computadoras, no sin antes destacar él Internet; una vía de comunicación efectiva y eficaz, donde nos une a todos por medio de una computadora.

Utilizando la Red de Área Local en una estructura interna y privada en una organización, seguidamente se construye usando los protocolos TCP/IP. Permite a los usuarios trabajar de una forma sencilla y efectiva, al mismo tiempo brinda seguridad en cuanto a la información ya que esta protegida por firewall: combinaciones de hardware y software que solo permite a ciertas personas acceder a ella para propósitos específicos.

Por otra parte el Intranet nos permite trabajar en grupo en proyectos, compartir información, llevar a cabo conferencias visuales y establecer procedimientos seguros para el trabajo de producción.

La Intranet es una red privada, aquellos usuarios dentro de una empresa que trabajan con Intranet pueden acceder a Internet, pero aquellos en Internet no pueden entrar en la Intranet de dicha empresa. El software que se utilizan en los Intranets es estándar: software de Internet como él Netscape, Navigator y los Navegadores Explorer para Web de Microsoft, facilitan en intercambios de información entre varios departamentos para poder llevar a cabo sus objetivos. Los programas personalizados se construyen frecuentemente usando el lenguaje de programación de Java y el guión de C.P.I. (Interfaz Común de Pasarela) permitiendo hacer negocios en línea, la información enviada a través de una Intranets alcanza su lugar exacto mediante los enrutadores.

Para proteger la información corporativa delicada las barreras de seguridad llamadas firewall (esta tecnología usa una combinación de enrutadores, que permite a los usuarios e Intranet utilizan los recursos de Internet, para evitar que los intrusos se introduzcan en ella).

Construyendo los protocolos TCP/IP (son los que diferencian a la Intranet de cualquier otra red privada) las cuales trabajan juntos para transmitir datos. (TCP: Protocolo de Control de Transmisión y el I.P: Protocolo de Internet), estos protocolos manejan el encadenamiento de los datos y asegura que se envían al destino exacto, funciona conjuntamente y se sitúan uno encima de otro en lo que se conoce comúnmente Peta de Protocolo, esta formatea los datos que se están enviando para que la pila inferior, la de transporte, los pueda remitir.

Cuando hay una gran cantidad de tráfico en una Red de Área Local, los paquetes de datos pueden chocar entre ellos, reduciendo en eficacia de la Red. Por tal motivo se utilizan combinaciones de Hardware y Software denominados Puentes que conectan con enrutadores en un solo producto llamado router, que ejecuta la tarea de ambos. Los enrutadores son los que aseguran que todos los datos se envíen donde se supone tienen que ir y de que lo hacen por la ruta más eficaz, desviando él trafico y ofreciendo rutas, cuentan con dos más puertos físicos. Los de recepción (de entrada) y los de envío (de salida), cada puerto es bidireccional y puede recibir o enviar datos.

Saliendo un poco en cuanto a Procesamiento de Datos podemos destacar dentro del Intranet el Uso de Correo Electrónico, utilizando a la vez el Protocolo Simple de Transmisión de Correo (CMTP), emplea una arquitectura cliente / servidor; el receptor del correo puede utilizar ahora un agente usuario de correo para leer el mensaje, archivarlo y responderlo. Frecuentemente el e-mail generado por Intranet no se entregará a una computadora de la Intranet, sino a alguien en Internet, en otra Intranet. EL mensaje deja la Intranet y se

envía a un enrutador Internet. EL enrutador examina la diversión, determina donde debería mandarse el mensaje, y después lo pone en camino.

El motivo por el cual una Intranet es porque a Web facilita la publicación de la información y formularios usando el Lenguaje de Hipertexto (HTML), permite también la creación de paginas iniciales multimedia, que están compuestas por textos, video, animación, sonido e imagen.

Los programadores pueden vincular datos corporativos desde una Intranet, permitiendo el uso de sistemas patrimoniales como base de datos en el Java, el cual es similar al lenguaje informático C++, es compilado, lo que significa que después de que el programa Java se escribe, debe ejecutarse a través de un compilador para transformar el programa en el lenguaje que pueda entender la computadora.

La Intranet se puede subdividir en varios niveles al momento de sobrepasar su tamaño y al ser difícil de manejar, para resolver el problema se crea subsecciones de una Intranet que las hacen más fáciles de hoslid: los bits que se usan para distinguir subredes se llaman números de subred.

Al mismo tiempo la Intranet cuenta con firewall que es la combinación de hardware / software que controla el tipo de servidores permitidos hacia o desde la Intranet, esta línea de defensa es por los ataques de aquellas personas que tengan el propósito de destruir o robar datos en una empresa ya que la Internet se expone a este tipo de ataques. Otra manera de emitirlos es usando un enrutador para filtrar, encaminar la dirección IP, y la información de cabecera de cada paquete que entra con la Intranet y solo permite el acceso aquellos paquetes que tengan direcciones u otros datos, que el administrador del sistema ha decidido previamente que puedan acceder a la Intranet.

Seguidamente para asegurar una Intranet se debe usar la encriptación el cual se utiliza para almacenar y enviar contraseñas o códigos específicos para asegurase que ninguna persona pueda entenderla. La clave es el centro de la encriptación. Las contraseñas deben cambiar frecuentemente, que no sean adivinadas fácilmente y tienen que ser elaboradas por personas autorizadas.

Por otra parte tenemos los vienes en la Intranet, son el mayor riesgo en la seguridad, pueden dañar datos, ocupar y consumir recursos e interrumpir operaciones. Estos virus se esconden dentro de un programa, hasta que no se ejecute ese programa el virus es inactivo, al ejecutarse entra en acción infectando en el disco duro copiándose de ellas. El software se ejecuta en un servidor de firewall para examinar al virus, también utiliza filtrado de paquetes, muy parecidos a lo que hacen los enrutadores para filtrar.

El software de supervisión simplemente deja pasar a los paquetes y sigue la pista a la información de los paquetes. Igualmente incluidos con el programa del servidor permite a los administradores de redes examinar y analizar él trafico de la Intranet y de Internet en un grado extraordinario. Algún software va más allá del análisis y permite a los administradores de Intranets cambiar el tipo de acceso a Internet de los usuarios de la Intranet, basándose en el tráfico, uso y otros factores.

Finalmente podemos decir que las Intranets permiten a los empresarios que a sus empleados trabajen en grupo, tal motivo se debe al extenso aportado de programas para trabajo en grupo y admite que los usuarios empleen la conferencia visual, compartan documentos, participen en discusiones y trabajen juntos de otro modo, no solo para coordinar negocios y hacerlos más

eficaces, sino también como un lugar para hacerlo, recibir y rellenar pedidos de bienes y servicios.

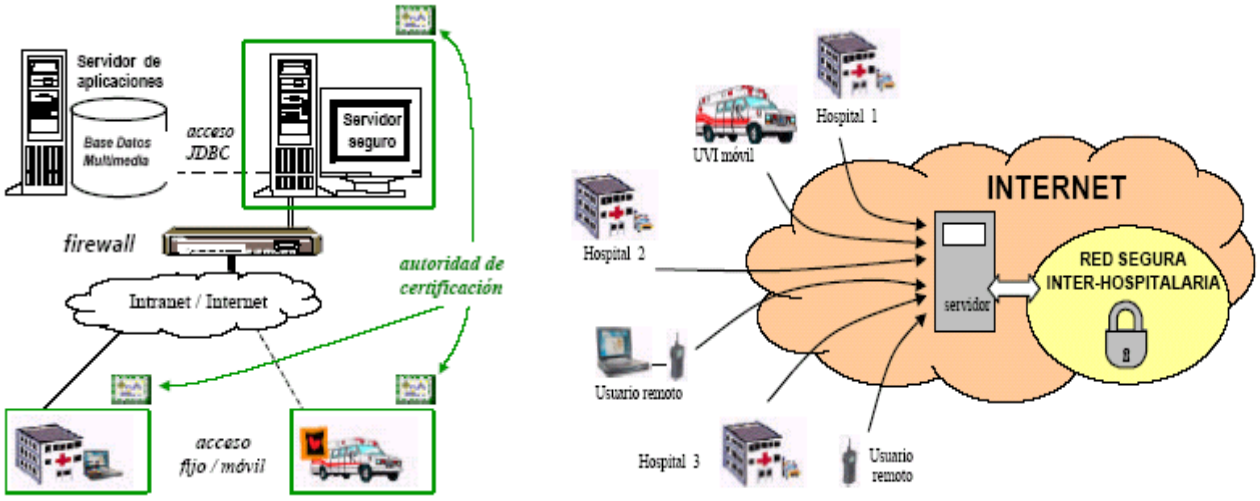



**Figura Nº 50 Modelo de una INTRANET / INTERNET Hospitalario**

# CAPITULO V

## DISEÑO PROPUESTO

En la primera parte se tratará la implementación de la infraestructura y en la segunda la implementación de los servicios.

Se incluyen los requisitos funcionales y técnicos del conjunto de instalaciones que necesitan de una red de comunicaciones para su funcionamiento.

Se realiza una aproximación al problema partiendo de un alto nivel de abstracción en el que se describen los servicios, con el fin de tener una visión de conjunto de los mismos así como su integración, llegando posteriormente a los sistemas que los soportan incluyendo niveles de detalle que permiten la concertación en procedimientos y productos susceptibles de ser usados en la ejecución del proyecto.

El objetivo es establecer los requerimientos funcionales y técnicos mínimos para la implementación de las instalaciones que requieren de una red de comunicaciones para su funcionamiento. En particular se consideran las instalaciones que proporcionan los siguientes servicios:

- Servicio de telefonía.
- Servicio de transmisión y comunicación de datos.
- Servicio de control de accesos, control de intrusión, y control de presencia.
- Servicio de Videoconferencia en salón de actos y aulas de formación.
- Servicio de sincronización horaria de todas las instalaciones.

## 5.1. Criterios generales para la implementación de la infraestructura

De la misma manera que la referencia para la actividad que se genera en un hospital alrededor de un paciente, debe ser el paciente (historia clínica unificada) y no los diferentes grupos operativos de producción que la generan (servicios médicos), el objetivo de todas las instalaciones que se describen en el presente proyecto deben tener como referencia el conjunto del hospital y no cada instalación en si misma. Esto implica que el nivel de integración debe ser máximo, por tanto los solapamientos en infraestructura y funcionalidad deben ser inexistentes o mínimos. Así, en la fase de redacción del proyecto de ejecución y en la fase de ejecución del mismo, se realizará un tratamiento de conjunto y se evitará el abordaje de las instalaciones a modo de islas, incluso, si esta consideración restringe el tipo de tecnologías o productos a usar.

El único requerimiento exigible es que sean conformes a estándares de facto o de norma en el ámbito de la industria.

El proceso de evaluación de alternativas, se tenderá a maximizar la siguiente expresión:

**Eficiencia = Prestaciones / Coste_ Generalizado**

Las prestaciones deben ser las requeridas para el buen funcionamiento del hospital y el coste generalizado debe considerar el coste de adquisición más el coste de mantenimiento y explotación.

El proyecto de ejecución se debe redactar asumiendo como filosofía general, que este tipo de instalaciones deben incorporar los siguientes principios:

- Toda instalación tiene que ser gestionable.
- Los servicios se deben poder conceder o retirar con criterios administrativos y nunca por restricciones técnicas.
- Los elementos de control y gestión de las diferentes instalaciones (salvo la de videoconferencia que es una instalación específica de locales concretos) deben estar concentrados en un único local, de acceso físico controlado, siendo posible su gestión desde dicho local o desde cualquier otro, con tal que se disponga de autorización suficiente.
- Los servicios que alojan la información de los diferentes subsistemas de información, que de forma integrada constituyen el sistema de información del hospital (tanto de su actividad como del propio), deben estar alojados en un único local con acceso físico controlado.
- Las redes de cableado necesarias para soportar las instalaciones descritas, deberán compartir la misma canalización principal, siempre que sean eléctricamente compatible entre sí.
- La topología física de las redes de transmisión a través de las cuales se soportan los diferentes servicios, será una estrella distribuida. Por tanto obedece a una estructura jerárquica, en la que partiendo de un Distribuidor Principal (MDF), se distribuye radialmente a los Distribuidores Secundarios (SDF) y desde estos, radialmente a los Puntos de Acceso a la Red de Transmisión en el edificio. No se permitirá ninguna conexión entre Distribuidores Secundarios (SDF) sin pasar por Distribuidor Principal (MDF), con el fin de eliminar bucles por diseño.

- La estabilidad de funcionamiento de los diferentes servicios se resolverá por diseño mediante las condiciones de contexto (estabilidad térmica y eléctrica) de la electrónica que soporta cada servicio, o mediante protocolos de supervisión de enlace, pero nunca por redundancia de electrónica que aumente desmesuradamente la complejidad de la gestión y funcionamiento de los mismos. En este sentido estas instalaciones no son distintas de cualquiera otras del hospital, por más que no estén consolidadas aún en la cultura tecnológica actual.

### 5.1.1. Diseño de las Redes de Cableado

La red de transmisión electrónica necesaria para soportar los diferentes servicios, es infraestructura de edificio al igual que la red de climatización o la red eléctrica y no de organización (personas que la ocupan), por tanto para su diseño se usará el mismo criterio que para el resto de instalaciones.

***Unidad de Servicio***

En la realización del diseño se usará un modelo que considera las siguientes variables:

- Inventario de ambientes (planos de arquitectura y mobiliario).
- Tipo de local (oficina , habitación, consulta, quirófano, UCI, etc.)
- Inventario de servicios necesarios en cada punto, para cada tipo de local.
- Densidad de puntos por unidad de superficie para cada tipo de local.

La topología de las diferentes redes de cableado desde los Puntos de Entrada a la Red de Transmisión Activa (Voz, Datos y video, etc.), será radial

hasta los Distribuidores Secundarios (SDF) y desde estos radial hasta el Distribuidor Principal (MDF), no estando permitido realizar ningún empalme en los conductores que se usen para su ejecución.

AL equipotencialidad eléctrica de las diferentes redes de cableado del edificio (sobre las que operan diferentes técnicas de señalización) se resolverá por diseño para cada distribuidor secundario, eliminando de esta forma los problemas de adaptación de impedancias, o lo que es lo mismo, garantizar por diseño la escabilidad de funcionamiento de las técnicas de señalización.

### 5.1.2. Ejecución del Cableado

Se utilizará tecnología de cableado integral estructurado para la ejecución de las diferentes redes que se abordan.

Para unir el Punto de Entrada a la Red de Transmisión Activa con el distribuidor secundario se usarán tantos mazos de cable distintos, como técnicas de señalización para las que se incorpore conector. El número de mazos depende de la configuración del Punto de Entrada a la Red de Transmisión Activa, siendo el caso general:

- 01 mazo de 4 pares de cobre de categoría 5E o 6 ampliada no apantallada para voz.
- 02 mazos de 4 pares de cobre de categoría 5E o 6 ampliada no apantallada para datos.
- 01 hilo de cobre flexible de 2,5 $mm^2$ amarillo-verde para tierra, 750 V aislamiento.
- 02 hilos de cobre flexible o rígido de 2,5 $mm^2$ marrón y azul para alimentación eléctrica 750 V aislamiento.

Para la conexión de todos los cables del mismo tipo, se usará el mismo tipo de herramienta.

La jerarquía de conexión es como se detalla en el siguiente esquema: Los mazos conductores de energía eléctrica en ningún caso y bajo ningún concepto compartirán canalización con los conductores de Voz, Datos, y video. Al Punto de Entrada a la Red de Transmisión Activa se llega con doble canalización. No estará permitida la canalización en derivación desde los Puntos de Entrada a la Red de Transmisión Activa para los servicios (datos, voz, video, etc.) ni para energía eléctrica.

### 5.1.3. Cuartos de Instalaciones

Para la implementación de los servicios que se abordan, son necesarios dos tipos de locales o cuartos de instalaciones:

- Cuartos de instalaciones para alojar la infraestructura de transmisión.
- Cuartos de instalaciones para alojar la infraestructura de los servicios.

Por razones de funcionalidad, control y seguridad en el acceso, es necesario que algunos de estos locales sean contiguos y estén en la misma planta. A este conjunto de locales les denominaremos Centro de Gestión Red (CGR).

**Cuartos de instalaciones para alojar la infraestructura de transmisión**

Para implementar la red de transmisión electrónica en el edificio, son necesarios dos tipos de locales en los que alojar el sistema de conexión y la electrónica que implementa la red:

- Distribuidor Principal (MDF)
- Distribuidor Secundario (SDF)

El Distribuidor Principal (MDF) es un local único para todo el hospital que conecta radialmente todos los Distribuidores Secundarios (SDF), más la electrónica que los une, constituye la troncal de la red de transmisión del hospital para cada uno de los sistemas que soportan los diferentes servicios.

Al ser los Distribuidores Secundarios (SDF), un mal necesario (por requerimientos técnicos de distancia) y no un bien deseable ya que habrá tantos puntos de administración de red y electrónica que incorporar como numero de Distribuidores Secundarios (SDF), el numero de ellos, será el menor posible. Este planteamiento es estrictamente compatible con una interpretación conceptual de la norma EIA/TIA 568B en materia de distribuidores de cableado:

CD : Distribuidor de Campus

BE : Distribuidor de Edificio

FD : Distribuidor de Planta

TP : Punto de Transición

Realizando un proceso de abstracción, se reduce el CD y BD al Distribuidor Principal (MDF), y el FD y TP al Distribuidor Secundario (SDF). De esta forma es posible superponer las normas EIA/TIA 568B y la norma IEEE 802.X, en particular el apartado que establece, que entre dos nodos, no puede haber más de dos repetidores (se considera en el peor caso, electrónica sin ningún nivel de inteligencia).

El modelo a usar para la ubicación de los Distribuidores Secundarios (SDF), consiste en superponer esferas de radio 90m sobre el edificio y desplazar asimétricamente los centros de las mismas a una única planta (si la

geometría del edificio lo permite), ya que esto minimiza el tiempo necesario para activar un servicio de red o revisar una disfunción, además garantizar la asepsia de las zonas limpias al no tener que acceder a las mismas para administrar servicios de red. La viabilidad de este planteamiento, se ve limitada por la geometría del edificio, siendo posible en hospitales.

***Cuartos de instalaciones para alojar los servicios***

Para implantar los servicios, son necesarios los siguientes locales o cuartos de instalaciones:

- Distribuidor Principal (MDF)
- Servidores
- Sistema de Alimentación Ininterrumpida
- Operadores de Sistema y Red
- Almacén para copias de seguridad
- Operadores de videoconferencia
- Área de informática y comunicaciones

### 5.1.4. Central de Gestión Red (CGR)

Al conjunto de locales de infraestructura de red o servicios, que deben ser contiguos en la misma planta, les denominamos Central de Gestión Red (CGR):

- Distribuidor Principal (MDF)
- Servidores
- Sistema de Alimentación Ininterrumpida
- Operadores de Sistema y Red

- Almacén para copias de seguridad

Los tres primeros están destinados a contener máquinas y no personas, por lo tanto se debe evitar la presencia de las mismas por espacios de tiempo prolongados. La mejor forma de resolver esto por diseño, es calibrar los termostatos de estos 3 locales a una temperatura de 20ºC, que es ideal para minimizar la fatiga mecánica y electrónica de los componentes de los equipos, al tiempo que es suficientemente hostil como para garantizar la no presencia humana por tiempos prolongados. El local de Operadores de Sistemas y Red debe tener inspección visual mediante cristal (con barrera térmica) sobre el MDF y sobre los servidores.

Los tres primeros locales dispondrán de suelo técnico conductivo cuya estructura de anti-polvo. Dispondrá de una rampa de acceso. La estructura metálica del suelo técnico estará puesta a tierra de estructura (no de datos).

**Distribuidor Principal (MDF)**

El MDF es el local donde se concentran todas las comunicaciones del edificio (hospital) tanto internas como externas, para todos los servicios que se describen, por tanto, es el local que se aloja todos los elementos de las troncales de red (cableado y electrónica).

La ubicación de este local en el edificio depende del tamaño y geometría del mismo. En el caso en que todo el cableado del edificio se pueda abordar desde un MDF único, su ubicación se decide con ciertos criterios técnicos y se centrará axialmente en el mismo. En el caso en que por razones de distancia no se pueda abordar el cableado del edificio desde un único distribuidor

(edificaciones grandes), su ubicación se puede decidir con criterios administrativos, ello implica que no debe tener dependencia técnica con el mismo, por tanto se podrá ubicar en la parte más conveniente atendiendo sobre todo a criterios de control, pudiendo compartir espacio físico con uno de los Distribuidores Secundarios (SDF).

Este local deberá disponer de al menos un punto de drenaje de agua, para evitar el deterioro de los equipos electrónicos en caso de inundación por rotura de alguna conducción de la red de agua limpia o sucia. En el MDF se alojan:

- Distribuidor de cliente que conecta con el operador público de comunicaciones.
- Distribuidor Principal del cableado de voz del hospital (Central Telefónico).
- Distribuidor Principal del cableado de datos del hospital (Conmutador Principal).
- Red Intranet del hospital (conecta las diferentes redes IP).
- Red Internet (comunicación externa al hospital).
- Distribuidor Principal de videoconferencia del hospital.
- Distribuidor de tierra de datos para el ámbito del CGR.

Deberá estar constituido por tantos armarios rack de 19” unidos mecánicamente entre sí, como fuere necesario. Los armarios que alojen electrónica, deben incorporar (en su parte inferior) dos raíles de 10 enchufes conectadas a dos circuitos eléctricos provenientes de 2 mecanismos diferenciales distintos del cuadro de maniobra del Sistema de Alimentación Ininterrumpida.

Este requerimiento es para la conexión de las fuentes de alimentación redundantes de la electrónica.

Se deberá instalar un mueble biblioteca para almacenar manuales y documentación de administración de la redes de cableado y de toda la electrónica que se aloje en el MDF.

**Figura Nº 51 Equipamiento del Cuarto de Telecomunicaciones (Backbone)**

***Servidores***

En este local se ubicarán los servidores de datos del hospital independientemente de área funcional a la pertenezcan:

- Servidor de nombres para la red local del hospital (DNS) + Estafeta correo electrónico.
- Servidor de las bases de datos documentales de uso clínico (MEDLINE, COCHRANE, UpToDate, etc).
- Servidor de la base de datos de Gestión de Pacientes.
- Servidor de la base de datos de Gestión Clínica.
- Servidor de la base de datos de Gestión de Personal.

- Servidor de la base de datos de Gestión de suministros y control de stocks.
- Servidor de la base de datos de Laboratorio.
- Servidor de la base de datos de Imágenes (PACS/IMACS).

Se deberá instalar un mueble biblioteca para almacenar los manuales y documentación de administración de todos los sistemas.

***Figura Nº 52 Servidores – Base Datos (en el Backbone)***

**Cuarto del Sistema de Alimentación Ininterrumpida (SAI)**

Es este local se ubicará el Sistema de Alimentación Ininterrumpida (SAI) y el cuadro de maniobra que lo gestiona, desde el que se alimenta eléctricamente todo el CGR.

El aire frío se inyectará a la altura del suelo, con el fin de facilitar la evacuación del calor por convección hacia la canalización de retorno, que

estará en la parte superior. La circulación de aire será mediante circuito forzado.

Este local deberá disponer de al menos un punto de drenaje de agua para evitar explosión o deterioro en caso de inundación por rotura de alguna conducción de la red de agua limpia o sucia.

**Cuarto de Operadores de Sistema y Red**

Este cuarto alojará espacio para no más de 2 o 3 personas, que serán los responsables de operación tanto de la parte de red como de la parte de sistemas, para todos los servicios.

**Figura Nº 53 Operador de sistema y red (Backbone)**

**Cuarto Almacén de copias de Seguridad**

Este cuarto alojará al armario ignífugo para almacenar:

- Las copias de seguridad.
- Los kits originales de todo el software del hospital.

- Los documentos con las contraseñas de administración de todos los equipos del hospital.
- La llave maestra de todas las cerraduras de todos los locales de las presentes instalaciones.

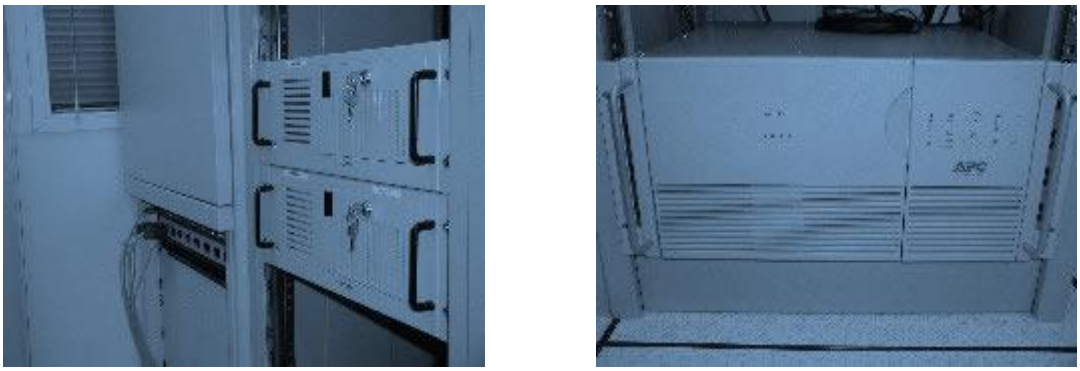


***Figura Nº 54  Sistemas de Seguridad Internas (Backbone)***

***Figura Nº 55  Sistemas de Seguridad Externas (Backbone)***

**Distribuidores Secundarios (SDF)**

Cuando por razones de distancia, no es posible abordar el cableado del edificio desde un distribuidor único (que es la situación ideal), son necesarios cuartos de instalaciones intermedias, denominadas SDF. Los locales de los SDF no requieren de suelo técnico (suelo falso).

**Cuarto de control de Videoconferencia**

En este local se alojará:

- Monitores de video conectados a la matriz de conmutación de video.
- Monitoreo de control de videoconferencia.
- Operadores de audio y video.
- Propiedades que deben incorporar los cuartos de instalaciones

***Seguridad en el Acceso***

Los locales del CGR y SDFs dispondrán de un Punto de Entrada a la Red de Transmisión Activa blindada con cerradura específica de seguridad y llaves maestras, así como paredes con dimensiones suficientes. Así mismo incorporarán terminal del sistema de control de accesos, que actuarán sobre el cerradero (sobre la cerradura seguirá actuando la llave), la alimentación eléctrica del mismo provendrá del SAI.

***Climatización***

Los siguientes locales:

- Distribuidor Principal (MDF).
- Servidores
- Cuarto de SAI.

Dispondrán de un sistema de climatización que sólo producirá frío, incluso en el caso en que la temperatura exterior al edificio sea superior a la del interior del mismo.

Aparte de la climatización con renovación de aire, incluirá baterías de apoyo con control de humectación.

El control del sistema será tal que se garantice su funcionamiento siempre que haya suministro eléctrico y la impulsión del aire frío se realizará por el falso suelo, lo que permitirá distribuir frío directo mediante rejillas a los servidores en los servidores y a los armarios en el MDF.

**Alimentación Eléctrica**

En el CGR se aloja electrónica que es crítica para el funcionamiento del hospital, por lo que debe ser alimentado eléctricamente desde una línea proveniente de un cuadro general del edificio y protegida por un grupo electrógeno en conmutación automática. Esta línea llegará a un conmutador de 3 posiciones (SAI, cero, línea) en el cuadro de maniobra del SAI, desde el que se alimentará a un sistema de Alimentación Ininterrumpida (SAI), cuya salida volverá al cuadro de maniobra en el que al tratarse de una fuente de energía autónoma, pasará por dispositivos diferenciales y desde éstos a los disyuntores magneto-térmicos bipolares que alimentarán los circuitos finales instalados en el CGR.

El SAI actuará como protector de sobretensiones y aislamiento galvánico en la alimentación a los equipos finales que soportan los servicios (servidores, conmutadores, enrutadores, etc.)

La tensión de salida del SAI estará referenciada a la tierra de datos, con el fin de garantizar el perfecto funcionamiento de la electrónica y de los mecanismos diferenciales.

En los Distribuidores Secundarios un SAI con la misma gestión y funcionalidad que en el Distribuidor Principal.

**Sistema de Tierra para la Red de Transmisión**

En toda red de transmisión en la que la técnica de señalización esté basada en variación de tensión eléctrica, es crítico para su funcionamiento la referencia o cero de la misma en el nodo emisor y en nodo receptor. Forma junto con la conexión, uno de los cuellos de botella en la implementación de una red de transmisión.

Para minimizar los problemas de perturbaciones no deseadas por una parte y aumentar el rendimiento de las fuentes de alimentación conmutada por otra, casi todos los equipos hacen coincidir el cero de la fuente de alimentación con el chasis de los mismos, por tanto, coincide la tierra lógica con la tierra física, que a su vez se conecta mediante el enchufe de energía eléctrica a la red de tierra asociada a la red de energía eléctrica. Para garantizar el funcionamiento en resonancia del circuito de la fuente de alimentación conmutada, resulta imprescindible controlar la frecuencia de la tensión de entrada, por esta razón las fuentes de alimentación incorporan un filtro que elimina a través de la línea de tierra los componentes distintos a 50Hz. Esta corriente de fuga (entre 60V y 80V en vacío) es la que provoca que nodos conectados a tierras con diferentes impedancias tengan comportamientos erráticos en la transmisión si la impedancia que ve un nodo a través de la línea de datos es menor que la que ve a través de la tierra de la red eléctrica.

El problema se plantea cuando en un edificio, un nodo conectado a la red de transmisión se alimenta eléctricamente de un punto cuya tierra tiene un valor de impedancia distinto al valor que tiene otro punto al que se conecta otro nodo en otra parte del edificio. Incluso este problema se plantea aunque la

transmisión se realice en modo diferencial, por las fugas a modo común de los "drivers" de línea, ya que en la práctica, o no es posible, o económicamente no es viable hacer equipos con aislamiento galvánico infinito.

Para resolver el problema descrito, lo mejor es optar por una solución agresiva, consistente en construir por diseño una superficie equipotencial asociada a la red de transmisión (o de datos). La implementación de esta superficie equipotencial se realizará mediante una red radial de tierra desde cada Distribuidores Secundarias a los Puntos de Entrada a la Red de Transmisión Activa que conecta en el edificio. A su vez esta red se mantendrá conectada / aislada con la red de tierra de baja tensión del edificio mediante vías de chispas, que pone en cortocircuito ambas redes por razones de seguridad frente a la caída del rayo.

El valor de resistencia medido en el conjunto de electrodos a la altura del terreno, previa desconexión de la cuchilla en la caja de corte y prueba (mediante instrumento: telurómetro apropiadamente calibrado), no será superior a 3 Ohmios.

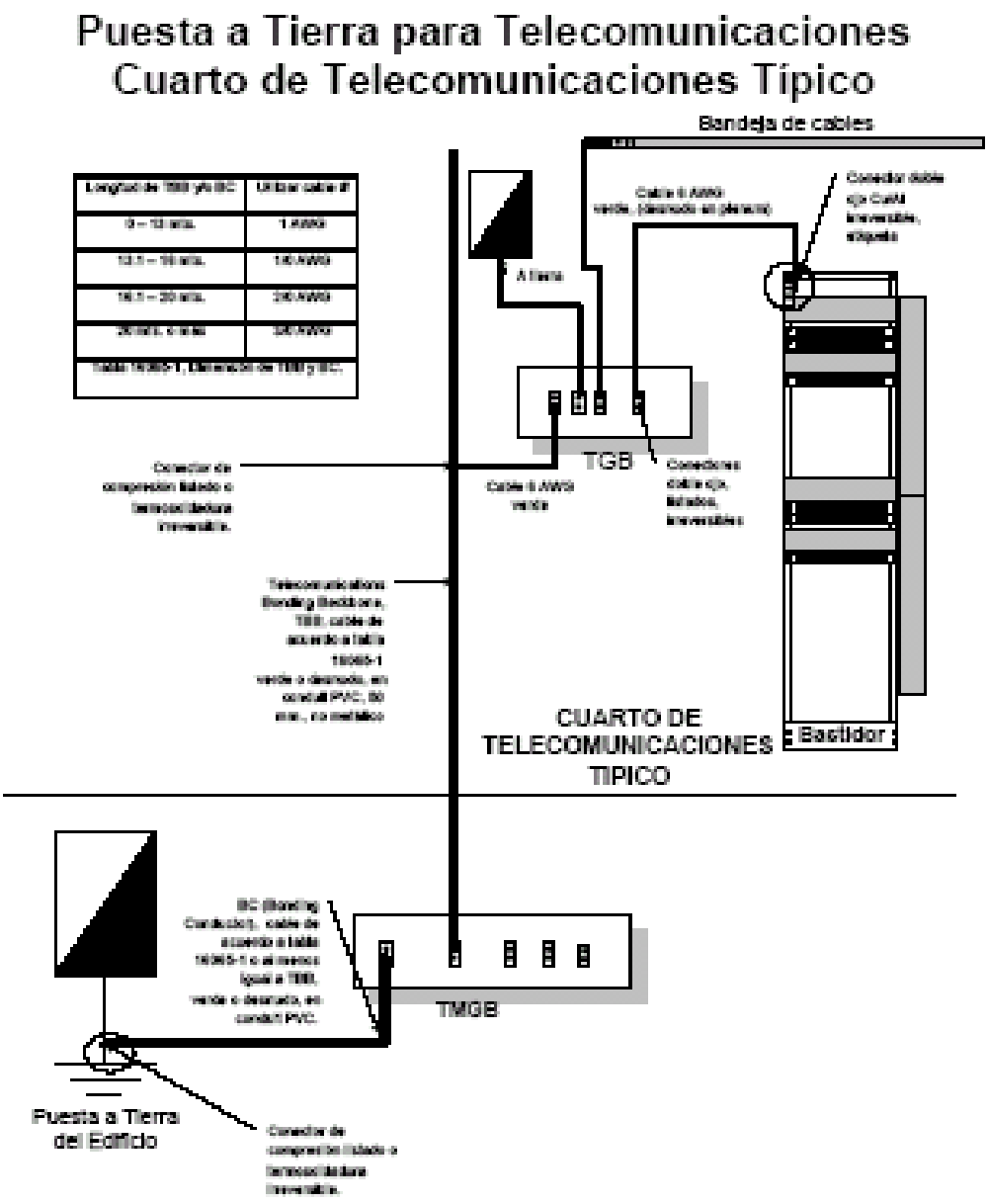



***Figura Nº 56  Sistemas Puesta a Tierra (Backbone)***

***Puntos de Entrada a la Red de Transmisión Activa***

Los servicios que se abordan, estarán disponibles para los usuarios a través de los Puntos de Entrada a la Red de Transmisión Activa (activa porque hace falta electrónica para que funcione), que constituyen los elementos finales de la red de transmisión.

En general los Puntos de Entrada a la Red de Transmisión Activa estarán basados en una caja de aluminio (que se comporta como jaula de Faraday) practicable, de dimensiones 362x176,4x66 mm (tipo Cymen de 12U o equivalente), empotrada en la pared. Su funcionalidad y configuración dependerá del local. Se establecen varios tipos:

- Propósito general **(CB+1V+2D)**
- Habitaciones de pacientes**(CB+2V+2D)**
- Granja de servidores**(CB+2D+2D+FO)**
- Aulas deformación **(CB+2D+2D)**
- Cabecera de las aulas de formación **(CB+1V+2D+MM)**
- Boxes de Urgencias, Reanimación, Cuidados Intensivos y Diálisis **(2D+FO)**
- Mostradores control enfermería en UCI **(CB+1V+2D+FO)**
- Quirófanos **(1V+FO)**
- Control de accesos **(2EE+1V+1D+BNC)**
- Televisión en RF**(2EE+1D+TV+FM)**
- Sólo telefonía, megafonía integrada y antenas DECT **(EE+1V)**

Descripción de los componentes del Punto de Entrada a la Red de Transmisión Activa:

**CB**: Todos los Puntos de Entrada a la Red de Transmisión Activa que incorporen este componente irán montados en cajas tipo Cymem o equivalente, con un conjunto de elementos comunes denominados **C**onfiguración **B**ase, constituidos por:

- Chasis metálico de aluminio empotrado en la pared (puesto a tierra de datos)
- Marco embellecedor de aluminio que se fija mediante tornillos al chasis (puesto a tierra de datos)
- Tapa frontal abatible con bisagras en sentido vertical en la que se alojan los mecanismos y conectores. Las bisagras la fijan al marco
- 1 Disyuntor magnetotérmico bipolar de 10 A
- Indicador luminoso (luz de neón) conectado a la salida del magnetotérmico.
- Enchufes de energía eléctrica redondos tipo shuco.
- Unidad central de ordenador personal / estación de trabajo.
- Monitor de ordenador personal.
- Impresora.
- Lámpara de mesa.
- En locales de dirección / gerencia se colocarán 6 enchufes para cargar teléfono celular.
- 1 Módulo de pre-conectorización eléctrica con tres bornas: neutro fase y tierra.

- 1 Placa metálica galvanizada para aislamiento de la parte eléctrica de la de voz y datos.

La conexión a la red eléctrica se realizará con cable de 2,5mm$^2$ rígido o flexible finalizado en Terminal tipo U. Se recomienda color azul para neutro y marrón para fase. La conexión radial de tierra al embarrado del Distribuidor Principal (MDF) / Distribuidor Secundario (SDF) se realizará mediante cable flexible de sección 2,5mm$^2$, 750V aislamiento, con funda de color amarillo-verde, estándar de instalación de energía eléctrica, finalizado en un Terminal tipo U, estañado (color plateado) fijado por presión mecánica y posteriormente soldado con estaño al conductor (por este orden) en el Puntos de Entrada a la Red de Transmisión Activa, y Terminal redondo en el embarrado de distribución radial de tierra en Distribuidor Principal (MDF) / Distribuidor Secundario (SDF), con el mismo procedimiento de conexión.

**1V**: Hace referencia a un conector RJ45 hembra categoría 5 ampliada, con conexionado por desplazamiento de aislante, enjaulado en un módulo de PVC que tiene serigrafiado en su parte superior un teléfono, insertable en el frontal de la caja, para acceso a la red de voz. La unión de este conector con el Distribuidor Secundario (SDF) será mediante 1 manguera UTP de 4 pares, categoría 5E o 6 ampliada.

**2V**: Hace referencia a dos conectores **1V**, enjaulados en el mismo tipo de módulo de PVC.

**2D**: Hace referencia a dos conectores RJ45 hembra categoría 5E o 6 ampliada, con conexionado por desplazamiento de aislante, trampilla frontal comandada por un muelle, que la mantiene cerrada si no tiene insertado ningún latiguillo y enjaulados en un módulo de PVC insertable en el frontal de la caja,

para acceso a la red de datos. La unión de estos conectores con el Distribuidor Secundario (SDF), será mediante 2 mangueras UTP de 4 pares, categoría 5E o 6 ampliada. Los Punto de Entrada a la Red de Transmisión Activas que incorporen este módulo, irá ubicado en el extremo de la caja lo mas lejos posible del disyuntor magnetotérmico.

**FO**: Hace referencia a dos conectores SC de Fibra Óptica multimodo 62,5/125mm, para acceso a la red de datos (o cualquier otro servicio disponible sobre Fibra Óptica). La unión de estos dos conectores con el Distribuidor Secundario (SDF) será mediante manguera blindada de 2 Fibras multimodo.

**MM:** Hace referencia a los conectores de audio y vídeo para conexión del equipamiento del puesto del docente, con el proyector de vídeo anclado en el techo (aulas o salón de actos). Estos conectores son:

- 01 VGA para conexión de la salida del adaptador de vídeo del ordenador.
- 02 RCA (color rojo y azul) para conexión del audio estéreo en formato ±100 mV, proveniente del adaptador multimedia del ordenador.
- 01 BNC para conexión de un magnetoscopio (salida de vídeo compuesto del euroconector).
- 02 RCA (color rojo y azul) para conexión del audio estéreo del magnetoscopio (salida de audio del euroconector).

**BNC:** Hace referencia a un conector BNC de 75 Ohmios unido al Distribuidor Secundario (SDF) mediante un cable RG59 de 75 Ohmios, 200 MHz, activo y malla estañados, para transportar la señal de vídeo en banda base proveniente de las cámaras de vídeo vigilancia.

**TV:** Hace referencia a un conector coaxial normalizado de 9 mm, 1dB, unido al Distribuidor Secundario (SDF) mediante cable coaxial de 75 Ohm,

2400 MHz, activo y malla estañados, para transportar la señal de TV en Radio Frecuencia. El activo del cable debe ser rígido y la malla debe cubrir al 100%.

**FM:** Hace referencia a un conector coaxial normalizado de 9 mm, 1dB, unido al conector de **TV** en el Punto de Entrada a la Red de Transmisión Activa mediante el filtro adecuado para obtener la señal de radio en Frecuencia Modulada.

**1EE**: Hace referencia a un enchufe de energía eléctrica, que usa tierra radial procedente del embarrado del Distribuidor Secundario (SDF). Este tipo de enchufe se utiliza en puntos de sólo voz y TV.

**2EE**: Hace referencia a dos enchufes de energía eléctrica de los definidos en **1EE.**

**Canalización**

La canalización es la infraestructura necesaria para el guiado y transporte de los cables. Se identifican 3 componentes:

- Canalización vertical, para guiado de cables en patinillos verticales del edificio.
- Canalización horizontal, para guiado de cables en planta.
- Canalización de acceso, para guiado de cables desde la canalización horizontal hasta el Punto de Entrada a la Red de Transmisión Activa.

Todos los Puntos de Entrada a la Red de Transmisión Activa incluyen una canalización que transporta los cables hacia el Distribuidor Secundario (SDF). Existen tres tipos de Punto de Entrada a la Red de Transmisión Activa que además de esta canalización, incluyen canalizaciones adicionales:

Puntos de control de accesos **(2EE+1V+1D+1BNC)**. Este Punto de Entrada a la Red de Transmisión Activa se instala por encima del falso techo y debe incluir canalización PG21 hasta:

- Cuadro eléctrico de planta para encendido de luces para grabación de cámara de vídeo.
- Cerco de la Punto de Entrada a la Red de Transmisión Activa para activación del cerradero y monitorización de cierre.
- Pared exterior al edificio para lector de tarjeta de control de accesos + control de presencia.
- Pared interior al edificio para lector de control de presencia.
- Punto de ubicación de cámara de vídeo en techo

Puntos de TV en habitaciones de pacientes **(2EE+1D+TV+FM)**. Este Punto de Entrada a la Red de Transmisión Activa se instala por encima del falso techo y debe incluir canalización PG21 hasta:

- Mueble cabecero de habitación de pacientes para control de volumen, conexión de cascos, control de canal, encendido y apagado del Televisor.

Puntos de cabecera de aulas de formación, **(CB+1V+2D+MM)**. Este punto se instala en la cabecera de las aulas a 30 cm a ejes del suelo y debe incluir canalización PG23 hasta:

- Falso techo del aula para conexionado de la parte multimedia (VGA+audio+vídeo+audio) con el proyector de vídeo fijado al techo.
- Pared frontal para alimentación del conmutador eléctrico de subir y bajar la pantalla de proyección.

En la instalación de la canalización tanto horizontal como vertical se evitará compartir el mismo patinillo o misma galería con:

- Tendido de distribución de energía eléctrica.
- Canalización de impulsión o retorno de la climatización.

Para minimizar la contaminación electromagnética producida por el efecto condensador y el efecto tribo-eléctrico producido por la canalización de climatización, se debe cortocircuitar la parte interna y la parte externa de los conductos de impulsión a distancias de 2 m y se debe adjuntar un conductor de cobre desnudo de 35 $mm^2$ que debe estar puesto a tierra de estructura por un extremo. Igual tratamiento se realizará con la canalización de retorno. Este criterio se debe respetar en las zonas de convivencia con la canalización de la red de transmisión.

Se respetará una distancia mínima de 1m para valores de tensión de 220 V o 380 V, con consumos de 15 a 100A. En el caso de cruces en galerías, la distancia mínima será de 40 cm. Igualmente se respetará esta distancia para la instalación de lámparas fluorescentes en cualquiera de las tres canalizaciones.

**Canalización Vertical**

La canalización vertical se realizará mediante bandeja metálica ranurada con tapa, galvanizada en caliente, sujeta en el platinillo vertical mediante distanciadores, tal que permita la fijación vertical de los mazos de cables mediante bridas de plástico. Sus perforaciones y remates deben ser de un tamaño lo suficientemente pequeño para que no puedan acceder los roedores.

Además se fijará a la misma (por su interior) a lo largo de su recorrido, un cable desnudo de cobre de 50 $mm^2$ mediante bridas metálicas y tornillos, a distancias de 2 m (si las piezas de bandeja fuesen inferiores a 2 m, se fijará como mínimo en un punto por pieza). Dicho conductor se pondrá a tierra de estructura (no de datos) por un extremo. Mediante lo establecido anteriormente, se le confiere al cableado a través de la canalización vertical las propiedades de:

- Antirroedor
- Apantallamiento frente a campo eléctrico

Se deberán cuidar los remates en la confluencia con la canalización horizontal, a fin de evitar superficies cortantes que puedan dañar los cables.

**Canalización Horizontal**

La canalización horizontal se realizará mediante el mismo tipo de instalación y bandeja que la canalización vertical.

La sujeción al techo incorporará los siguientes elementos (como mínimo) por punto de sujeción, a distancia de 1,5m como máximo:

2 varillas metálicas roscadas de 10 mm (longitud 50 cm)

2 tacos metálicos empotrados en el forjado del techo

1 tuerca que actúa como contratuerca entre la varilla y el taco metálico

1 tirante metálico fijado a la bandeja por su parte inferior mediante dos tornillos de cabeza plana (semiesférica) y fijado a las varillas roscadas mediante tuerca y contratuerca en los dos puntos (4 tuercas).

En su instalación, siempre que sea necesario realizar un cambio de dirección con un ángulo de 90º o inferior, el codo describirá por su parte mas interna un arco de circunferencia igual o superior a 50cm. Se fijará a la misma

(por su interior) a lo largo de su recorrido, un cable desnudo de cobre de 50 $mm^2$ mediante bridas metálicas y tornillos, a distancias de 2m (si las piezas de bandeja fuesen inferiores a 2m, se fijará como mínimo en un punto por pieza). El cable desnudo de cobre, se unirá por soldadura aluminotérmica al cable desnudo de cobre de la canalización vertical, que lo unirá a tierra de estructura en los Distribuidores Secundarios (SDFs).

**Dimensionamiento**

Para el dimensionamiento de la sección de las bandejas de la canalización horizontal y vertical, se tendrán en cuenta los diferentes tipos de cables que van a alojar y el diámetro exterior de cada tipo. Existe un modelo relativamente complejo, que se puede aproximar sin mucho error usando una bandeja de sección el doble de la sección de los cables que va a contener.

## 5.2. Criterios generales para la implementación de los servicios

La infraestructura de transmisión y comunicaciones de un hospital, es una de las instalaciones estratégicas para el funcionamiento del mismo en régimen de explotación. El objeto del proyecto es establecer los requerimientos funcionales y técnicos mínimos para la implementación de la infraestructura de transmisión y comunicaciones

En particular se consideran las instalaciones que proporcionan los siguientes servicios:

- Servicio de telefonía.
- Servicio de transmisión y comunicación de datos.
- Servicio de televisión.

- Servicio de control de accesos, control de intrusión, control de presencia y vídeo vigilancia.
- Servicio de videoconferencias en salón de actos y aulas de formación.
- Servicio de sincronización horaria de todas las instalaciones

**Servicio de Voz**

Se agrupan bajo este epígrafe todos los servicios que requieren comunicación vocal para su funcionamiento. El objetivo es integrar el máximo número de servicios sobre la misma tecnología, con el fin de facilitar el uso y minimizar los costes de mantenimiento y explotación.

Para la implementación de los servicios, existen en este momento dos tecnologías:

- El sistema de telefonía convencional basado en una centralita telefónica digital.
- Voz sobre protocolo IP (VoIP) que es una tecnología muy incipiente.

La tecnología convencional aporta esencialmente la estabilidad de funcionamiento propia del tiempo que lleva en el mercado, por lo que es una tecnología madura y muy depurada. Todos los operadores públicos de telefonía facilitan el servicio de comunicación vocal sobre este tipo de tecnología. Por contra está basada en sistemas propietario, incompatibles entre fabricantes (no a nivel de enlaces, sino a nivel de extensiones que no sean analógicas o digitales RDSI).

La incipiente tecnología de VoIP aporta la gran ventaja de que comparte la misma red y electrónica que la red de transmisión de datos y el mismo sistema de gestión de red. El sistema que gestiona la señalización y el nivel de

servicio, "gatekeeper", funciona sobre plataforma estándar de la industria tipo UNIX / Windows NT.

La tecnología que se propone en el presente proyecto, estará basada en una centralita telefónica digital que soporte VoIP.

**Servicio de Red**

Usando como tecnología base la centralita telefónica, se implantarán los siguientes servicios:

- Servicio de telefonía
- Servicio de intercomunicación
- Servicio pase espere de consultas externas

Todos estos servicios se implementarán usando la centralita telefónica y variando el tipo de terminal (teléfono) o la forma de comunicarse con el mismo.

**Servicio de Telefonía**

El servicio de telefonía permitirá la comunicación vocal telefónica dentro del edificio y con el exterior.

Se puede considerar que hay dos tipos de servicio:

- Servicio de telefonía sin pre-pago.
- Servicio de telefonía con pre-pago.

El servicio de telefonía sin pre-pago se aplicará con carácter general a:

- Todo el tráfico interno al hospital.
- Todo el tráfico entrante al hospital.
- Todo el tráfico saliente de personal autorizado del hospital.

El servicio de telefonía con pre-pago se aplicará con carácter general a:

- Todo el tráfico saliente del hospital procedente de habitaciones de pacientes.
- Todo el tráfico saliente del hospital procedente de teléfonos públicos

Los terminales telefónicos a usar en el hospital, serán digitales con "display" para ver el identificador de la llamada entrante. Incluirán soporte para dos extensiones (dos llamadas simultáneas), función de manos libres e indicador luminoso que avise de la existencia de correo de voz pendiente de escuchar.

**Servicio de intercomunicación**

El servicio de intercomunicación permitirá la comunicación vocal dentro del edificio en paralelo con el servicio de telefonía, de hecho es un servicio de telefonía con 2 canales de comunicación en cada Terminal telefónico.

Es un subconjunto del servicio de telefonía, por tanto, se usará la misma tecnología e infraestructura que para el servicio de telefonía. Su implementación requerirá que los terminales telefónicos, puedan operar en manos libres y que tanto la centralita como los terminales telefónicos soporten dos extensiones sobre el mismo Terminal (Terminales Multilínea).

Hay un caso particular de intercomunicación con las Punto de Entrada a la Red de Transmisión Activas que llevan asociado sistema de control de acceso, en el que se requiere un terminal (teléfono) con un único pulsador, que al pulsarlo provoca el marcado de la extensión del operador del sistema de control de accesos.

***Servicio pase espere de consultas externas***

El servicio de pase espere permitirá el aviso por megafonía a los pacientes en espera de acceder a los gabinetes de consultas externas. Funcionará de forma selectiva sobre un altavoz situado en el falso techo sobre la Punto de Entrada a la Red de Transmisión Activa de la consulta y diferentes altavoces situados en las diferentes salas de espera de consultas externas.

Es una modalidad del servicio de telefonía. Se usará la misma tecnología y centralita telefónica del servicio de telefonía y en los puntos finales, terminales telefónicos con funcionalidad de descolgado automático, "ding-dong" de llamada de atención, capacidad de ajuste del nivel de volumen de forma individual para el altavoz, indicador luminoso intermitente sobre el altavoz (llamada de atención de discapacitados auditivos) y colgado automático de la llamada por silencio.

El acceso se realiza marcando la extensión de destino o configurando el contenido de dos teclas de función en los terminales telefónicos tal que una provoque la llamada a la extensión del altavoz de encima de la Punto de Entrada a la Red de Transmisión Activa y la otra, a la extensión de cabecera de un grupo de extensiones que incluye las salas de espera.

**Red de Cableado de Voz**

Es la red que va a soportar todos los servicios de comunicación vocal que se apoyan en la centralita telefónica.

| | |
|---|---|
| **Entrada** | Extensiones provenientes de la<br>Centralita Telefónica. |
| **Salida** | Mangueras de 100 pares de la troncal<br>de voz del edificio.<br>Conectores de antenas para terminal<br>DECT. |

**Arquitectura de la Red de Cableado**

La arquitectura de la red física es una estrella distribuida, en la que se distinguen dos componentes:

- Red Vertical o troncal basada en mangueras de 100 pares entre el Distribuidor Principal (MDF) y los Distribuidor Secundario (SDFs).
- Red Horizontal o capilar de voz basada en mangueras de 4 pares entre los Distribuidor Secundario (SDFs) y el Punto de Entrada a la Red de Transmisión Activa.

**Red Vertical o Troncal de Voz**

La Red Vertical o troncal de voz estará formada por las mangueras de 100 pares de cobre que unen el Distribuidor Principal de voz en el Distribuidor Principal (MDF), con los Distribuidores Secundarios de voz en los Distribuidor Secundarios (SDFs).

Estas mangueras serán de cable de par trenzado sin apantallar, 100 pares, categoría 5E o 6 con impedancia característica 100 Ohmios.

***Red Horizontal o Capilar de Voz***

La Red Horizontal o capilar estará formada por mangueras de 4 pares trenzados sin apantallar, que unen el Punto de Entrada a la Red de Transmisión Activa en el edificio con los Distribuidores Secundarios de voz en los Distribuidores Secundarios (SDFs).

Debido a que tanto los actuales terminales telefónicos analógicos (3KHz), terminales telefónicos digitales RDSI acceso básico (2B+D) 64+64+16 Kbs, incluso los futuros terminales de voz sobre IP (10 Mbps) pueden operar sobre un medio de transmisión que soporta 10 Mbps, sería suficiente usar cable de categoría 3, sin embargo se opta por categoría 5E o 6 ampliada, porque la diferencia de costo no justifica el inmovilizado que sería necesario tener en la fase de acopio de materiales y porque al no ser una tecnología totalmente consolidada por falta de cultura tecnológica, se pierde más tiempo en explicar porqué sólo se requiere cable de categoría 3, que poner el mismo tipo de cable que para la red de datos.

**Componentes Pasivos**

- Manguera de 4 pares trenzados de cobre sin apantallar, categoría 5E ampliada entre el Distribuidor Principal (MDF) y el Punto de Entrada a la Red de Transmisión Activa en el edificio.
- Manguera de 1 par trenzado de cobre sin apantallar, categoría 3, para el parcheo entre el cableado troncal y el cableado capilar en los

Distribuidores Secundarios (SDFs) y para el parcheo entre el cableado troncal y la centralita telefónica en el Distribuidor Principal (MDF).

- Módulos de conexionado de 4x25 pares tipo M110, para el conexionado de las mangueras de 100 pares del cableado troncal usando galletas de 5 pares y para el conexionado de las mangueras de 4 pares del cableado capilar, usando galletas de 4 pares.
- Módulos guía-cables para intercalar entre los módulos soporte de conexionado de 4x25 pares.
- Galletas de 5 pares categoría 3, para el conexionado del cableado troncal sobre módulos 110 tanto en el Distribuidor Principal (MDF) como en los Distribuidores Secundarios (SDFs).
- Galletas de 4 pares categoría 5E ampliada, para el conexionado del cableado capilar sobre módulos 110 en los Distribuidores Secundarios (SDFs).
- Módulos RJ45 hembra categoría 5E ampliada, para empotrar en módulo soporte de PVC en la caja que implementa el Punto de Entrada a la Red de Transmisión Activa.

**Componentes Activos**

Los componentes activos de la red de voz están formados por:

- Centralita telefónica.
- Terminales telefónicos.
- Módem externo de Telemantenimiento.
- Tarificador de tráfico saliente.
- Subsistema de tarificación pre-pago integrado Telefónico.

**Centralita Telefónica**

El sistema de telefonía a instalar en el edificio, estará homologado por la Empresa Telefónica del Perú SAA. La centralita telefónica a instalar será digital y deberá cumplir con los siguientes requerimientos funcionales mínimos:

- La centralita debe ser digital de última generación.
- Deberá ser capaz de soportar como mínimo tantos puertos como extensiones requiera el hospital.
- Se alimentará a 220V, 50 Hz.
- Incluirá funcionalidad redundante (a nivel de procesador).
- La arquitectura para conexión de módulos, debe ser de bus.
- El control se realizará mediante programación en base a "software" actualizable.
- El software a suministrar para su funcionamiento se considerará como una única unidad a los efectos de número de licencias, es decir todos los módulos deberán tener el mismo número de licencias. Debe incorporar soporte para VoIP.
- Debe incluir todos los paquetes de software necesarios para el correcto funcionamiento de la centralita en régimen de explotación.
- Debe incluir el software necesario para que funcionando sobre plataforma estándar UNIX / Windows conectado por red local Ethernet con la centralita, permita configurar, gestionar y mantener la centralita.
- Debe incluir soporte para 16 enlaces analógicos sin tele cómputo con el nodo frontal del operador público de telefonía, para funciones de "back-up".

- Debe incluir soporte para tantos enlaces RDSI acceso primario como el 12% de todas las extensiones con salida al exterior, módulo 30.
- Debe incluir soporte para tantas extensiones digitales como la suma de todos los terminales telefónicos de locales ocupados de forma habitual por personal del hospital.
- Debe incluir soporte para tantas extensiones analógicas como la suma de:
    - Terminales telefónicos de habitaciones de pacientes.
    - Terminales telefónicos de pase espere de consultas externas.
    - Terminales telefónicas de aviso por megafonía.
- Debe incluir soporte para tantas extensiones y antenas de radio de telefonía inalámbrica DECT como la suma de terminales celulares necesarios para cubrir la funcionalidad del hospital.
- Incluir soporte de correo de voz para un número de buzones igual a la suma de todos los teléfonos digitales y teléfonos DECT. El número de canales simultáneos debe ser igual al 50% del valor de pico de las llamadas concurrentes entrantes que tienen un identificador directo entrante (nº directo visto desde el exterior). Se asume que un 50% no descuelgan el terminal. En ningún caso será inferior al 16% del número de canales B con el operador público de telefonía, con un tiempo de grabación de 10 minutos por buzón.
- Debe incluir 4 canales de señalización E&M para conexión con fuente musical (música en espera).

- La conexión de las antenas DECT deberá ser mediante cable UTP categoría 5E ampliada y la alimentación eléctrica de éstas, debe ser local a 220 V, 50 Hz.
- La conexión de los terminales (teléfonos) tanto analógicos, como digitales debe ser a 2 hilos.
- Debe incluir 2 puestos específicos de operadora, con micrófono y cascos.
- Debe incluir operadora automática (mensaje pregrabado).
- Debe incluir música en espera.
- La gestión de la centralita de forma local o remota, se realizará exclusivamente por interfases propias de informática y no de telefonía. Por tanto sólo se admiten como interfases para este propósito RS232C asíncrona y 10Base-T ó 100Base-TX.
- Debe incluir 3 puertos tipo RS232C para:
    - Conexión de terminal de configuración inicial en local.
    - Conexión de impresora / tarificador para imprimir / capturar información de tarificación.
    - Conexión mediante módem de un terminal remoto para Telemantenimiento.
- Debe incluir 1 puerto Ethernet 10/100Base-TX para comunicación con el software de configuración, mantenimiento y gestión de la centralita.
- Debe incluir la documentación completa necesaria para desarrollar aplicaciones que interactúen con la centralita. Por tanto debe facilitar tanto las APIs (Aplication Program Interfaces) como las librerías de funciones primitivas de servicio, entorno de desarrollo y programación

para este propósito. Este requisito es imprescindible para la implementación del sistema de tarificación pre-pago integrado de telefonía.

- La centralita se debe conectar al Distribuidor Principal de voz en el Distribuidor Principal (MDF), mediante mangueras de 25 pares acabadas en conector TELCO en la centralita y parcheadas en los paneles 110 en el Distribuidor Principal (MDF).
- La centralita se debe conectar a enlaces provenientes de un nodo frontal del operador público de telefonía que sea digital, ya que solo deberá incorporar detector de tonos para esta señalización.
- Los enlaces analógicos de "back-up" a contratar con el operador público de telefonía deben incluir la siguiente funcionalidad:
    - Marcación por multifrecuencia.
    - Función de supervisión (inversión de polaridad al colgar el teléfono llamante).
- Todos los enlaces deben pasar por dispositivos de protección contra fenómenos atmosféricos (descargadores de sobretensiones) antes de conectarse a la centralita.

**Terminales Telefónicas**

Son necesarios los siguientes tipos de terminales telefónicos:

- Terminales digitales para el servicio de telefonía sin pre-pago del personal del hospital (se recomienda que sean todos iguales). Las especificaciones funcionales mínimas son:
    - Conexión con la centralita a 2 hilos.

- Formato de sobremesa o anclaje en pared.
- Multilínea (2 extensiones).
- Display de LCD de mínimo 2 líneas de 24 caracteres, para presentar hora, duración de la conversación actual e identificador de llamada entrante.
- 7 teclas programables para prestaciones (transferir llamada, conferencia, escuchar correo de voz, desvío, no molesten, etc.) con indicación luminosa de su activación.
- Indicador luminoso de mensaje pendiente de escuchar en el correo de voz.
- Teclas de retención de llamada y desconexión.
- Funcionamiento manos libres: operación con microteléfono colgado.
- Inhibidor de micrófono.
- Control de volumen independiente para microteléfono y altavoz.

- Terminales analógicos para el servicio de telefonía sin pre-pago en cuartos de instalaciones. Deben ser analógicos para que permitan la conexión de equipos de instrumentación y medida que puedan ser operados de forma remota (vía módem). Las especificaciones funcionales mínimas serán:
    - Conexión con la central a 2 hilos.
    - Marcación por multifrecuencia.
    - Tecla de rellamada.
    - Formato de sobremesa o anclaje en pared

- Terminales analógicos para el servicio de telefonía con pre-pago en habitaciones de pacientes. Se pone analógico para permitir la conexión con sistema de tarjeta monedero. La integración del terminal telefónico con el lector de la tarjeta monedero, debe ser compacta y formar un conjunto estéticamente aceptable. Las especificaciones funcionales mínimas son:
    - Lector de tarjeta monedero.
    - Conexión con la central a 2 hilos.
    - Marcación por multifrecuencia.
    - Display LCD para visualizar número marcado y cantidad de dinero disponible en tarjeta.
    - Tecla de rellamada.
    - Formato de sobremesa o anclaje en pared
- Terminales analógicos para el servicio de pase espere y megafonía. Las especificaciones mínimas son:
    - Tipo partido electrónica y altavoz.
    - Conexión con la central a 2 hilos.
    - Descolgado automático por detección de llamada entrante y colgado por silencio de más de 4s.
    - Generación de "ding-dong" de llamada de atención.
    - Alimentación eléctrica local a 220V, 50Hz.
    - Ajuste de ganancia variable para regular el nivel sonoro del altavoz.
    - Indicador luminoso intermitente para llamar la atención a discapacitados auditivos

- Terminales analógicos para el servicio de interfonía asociado a las Punto de Entrada a la Red de Transmisión Activas con control de accesos. Las especificaciones mínimas son:
    - Terminal sin teclado, una única tecla que al pulsarla marca la extensión que tenga preconfigurada.
    - Conexión a la red de telefonía mediante conector RJ11.
    - Alimentación eléctrica local a 220V, 50Hz.
    - Ajuste de ganancia variable para regular el nivel sonoro del altavoz.
    - Indicador luminoso que señalice el establecimiento de la comunicación.
    - Colgado automático por silencio de más de 4s o por tiempo de funcionamiento.
    - Capacidad de configuración local del número de extensión a marcar.

**Tarificador**

Para conocimiento y control del gasto telefónico generado desde el hospital hacia el exterior, es necesaria la incorporación de un software de aplicación que capture la información de llamadas que genera la centralita telefónica, lo organice en una base de datos y permita generar informes agregados o desagregados por diferentes criterios. El software de tarificación incorporará la siguiente funcionalidad:

- Capturará en tiempo real la información de tarificación.
- Almacenará la información de tarificación de forma permanente.

- Permitirá configurar por el hospital el modelo de coste telefónico para determinar la facturación.
- Garantizará integridad de la BD ante un apagón del equipo.
- Generará informes de facturación por extensiones o grupos de ellas en intervalos de fechas.
- Incluirá un manual de usuario en el que aparte de describir la operativa asociada a la funcionalidad, incluirá los siguientes extremos:
    - Descripción del diccionario de la Base de Datos (BD) que usa.
    - Procedimiento de importación / exportación de la BD.
    - Procedimiento externo que permita realizar Revisión de Integridad referencial de la BD.
    - Facilitará el modelo analítico de crecimiento de la BD en función del número de llamadas

**Servicio de Datos**

Se agrupan bajo este epígrafe los servicios de transmisión y comunicación de datos requeridos por las aplicaciones informáticas del hospital:

- Aplicaciones de gestión administrativa:
    - Contabilidad general, presupuestaria y analítica.
    - Suministros, compras y almacenes.
    - Ofimática
- Aplicaciones de gestión clínica:
    - Admisión de urgencias.

    - Admisión de hospitalización.
    - Archivo de historias clínicas.
    - Citaciones de consultas externas.
    - Informes de alta y codificación.
    - Facturación

- Aplicaciones departamentales:
    - Gestión de Quirófanos.
    - Gestión de Enfermería.
    - Gestión de Radiología e imagen (PACS/IMACS).
    - Gestión de Laboratorios.
    - Gestión de Farmacia.
    - Gestión de Anatomía Patológica.
    - Gestión de Nutrición y cocina.
    - Gestión de Servicios Generales y mantenimiento.
    - Monitorización y Control de Pacientes en UCI.
- Aplicaciones de productividad del personal clínico en servicios médicos:
    - Gestión de Bibliografía.
    - Gestión y Control de equipos de Instrumentación Clínica para ejecución de pruebas.
    - Videoconferencia.
- Acceso a documentación, bibliografía y formación continuada:
    - Base de Datos Medline, Cochrane, Courrent Contents, etc.
    - Servidor de vídeo con seminarios, cursos, etc.
    - Acceso a internet

Los componentes que dan soporte a este servicio son:

Red de Cableado.

Electrónica de concentración o conmutación en los Distribuidores Secundarios (SDFs).

Electrónica de conmutación y comunicación interna al hospital en el Distribuidor Principal (MDF).

Electrónica de comunicación externa al hospital en el Distribuidor Principal (MDF).

El conjunto formado por la red de cableado más la electrónica de concentración o conmutación, constituye la red de transmisión de datos del hospital.

El conjunto formado por la red de transmisión de datos del hospital más la electrónica de comunicación interna al mismo, constituye la intranet del hospital.

El conjunto formado por la electrónica de comunicación y los enlaces a través de los cuales se conecta el hospital con los centros de salud de su área sanitaria constituye la intranet del hospital. En esta electrónica es donde se deben implantar las reglas de seguridad para el acceso desde el exterior a los servidores que alojan los datos sensibles.

**Servicios de Red**

La red de comunicación del hospital conectará todos los ordenadores entre sí, con filosofía de:

- Bases de Datos centralizadas y únicas (no se considera la replicación potencialmente necesaria a nivel central para maximizar el rendimiento de las aplicaciones).
- Proceso distribuido.

Se asume que las plataformas que se instalarán en materia de sistema operativo y comunicaciones serán:

- LINUX sobre nodos Cliente o Servidor.
- UNIX (GPOS XPG3/4 de X/Open) sobre nodos servidor.
- WINDOWS 95/98 sobre nodos cliente.
- WINDOWS NT sobre nodos cliente o servidor.
- Familia de protocolos TCP/IP en todas las plataformas, como extensión de las mismas.

Los servicios se prestan mediante un conjunto de reglas y procedimientos denominados protocolos. A continuación se enumeran los servicios de red más relevantes y los protocolos con los que se deben prestar, se observa en la siguiente tabla:

Tabla Nº 03 Protocolos que se usan según el servicio hospitalario

| SERVICIO DE RED | PROTOCOLO | ÁMBITO DE APLICACIÓN |
|---|---|---|
| Sistema de ficheros distribuido | SMB | Intranet |
| Sistema de ficheros distribuido | NFS | Intranet |
| Terminal virtual | telnet | Intranet / Internet |
| Transferencia de ficheros | ftp | Intranet / Internet |
| Correo electrónico | POP3/SMTP | Intranet / Internet |
| Impresión remota | Lpr | Intranet |
| Gestión de red | SNMP, RMON | Intranet |
| Distribución de tiempo | NTP, SNTP, XNTP | Intranet / Internet |
| Transporte entre elementos finales | TCP/IP | Intranet / Internet |
| Comunicación entre procesos | Sockets | Aplicaciones cliente /servidor |

La columna **servicio de red** identifica las necesidades de los usuarios (en este caso los usuarios de la red de transmisión de datos, son los diferentes nodos constituidos por ordenadores que se interconectan a través de la misma).

La columna **protocolo** identifica bajo que reglas y procedimientos se soportan los servicios. Los protocolos seleccionados constituyen la familia de protocolos TCP/IP, que tienen la ventaja de ser independientes de fabricante y sistema operativo.

El **Ámbito de aplicación** identifica en qué red se garantiza la interoperabilidad de los protocolos:

- Intranet (red interna del hospital incluida la comunicación con los centros de salud del mismo área sanitaria).
- Internet (conexión con el resto del mundo).

**Red de Cableado de Datos**

Es la red que va a soportar todos los servicios de comunicación de datos entre los ordenadores servidores que alojan las bases de datos y la parte servidor de las aplicaciones, con los clientes que alojan la parte cliente de las aplicaciones usando la intranet del hospital.

Tabla Nº 04 Modo de distribución de la información

| | |
|---|---|
| **Entrada** | Conmutador de nivel 3 en el DISTRIBUIDOR PRINCIPAL (MDF) y conmutadores de nivel 2 en los DISTRIBUIDOR SECUNDARIO (SDF)s |
| **Salida** | Ordenadores servidores en la granja de servidores<br>Ordenadores cliente distribuidos por el hospital<br>Equipos de instrumentación clínica (autoanalizadores,<br>Equipos RX, etc.) |

El cableado de datos saldrá de forma radial del distribuidor de datos del Distribuidor Principal (MDF) a los Distribuidores Secundarios (SDFs) y desde éstos saldrá radial a los Puntos de Entrada a la red de Transmisión Activas

distribuidos por el hospital. Este cableado compartirá canalización con el resto de cableados de los servicios que se abordan en el presente proyecto.

### Arquitectura de Red

La arquitectura física de la red es una estrella distribuida, en la que se distinguen dos componentes:

- Red Vertical o Troncal de Datos.
- Red Horizontal o Capilar de Datos.

### Red Vertical o troncal de datos

La red troncal estará formada por las mangueras de fibra óptica que unen los Distribuidores Secundarios (SDFs) con el Distribuidor Principal (MDF). La razón de usar fibra óptica es para resolver los problemas de adaptación de impedancias en el edificio y la distancia.

### Red Horizontal o capilar de datos

La red horizontal o capilar de datos estará formada por las mangueras de 4 pares de categoría 5E ampliada que unen los conectores RJ45 de datos de los Puntos de Entrada a la Red de Transmisión Activas con los Distribuidores Secundarios (SDFs) y las mangueras de 2 fibras multimodo 65/125mm que unen los conectores SC de los Puntos de Entrada a la Red de Transmisión Activas (en locales con alimentación eléctrica de neutro aislado, tal como UCI, Reanimación, Quirófanos, Diálisis, etc.) con los Distribuidores Secundarios (SDFs).

**Componentes pasivos (cables y conectores)**

- Mangueras blindadas de 12 fibras ópticas multimodo 62,5/125mm entre los Distribuidores Secundarios (SDFs) y el Distribuidor Principal (MDF).
- Mangueras blindadas de 2 fibras ópticas multimodo 62,5/125mm entre los Puntos de Entrada a la Red de Transmisión Activas y los Distribuidores Secundarios (SDFs).
- Conectores SC para el conexionado de la Fibra Óptica.
- Bandejas cerradas de montaje en rack de 19 pulgadas para alojar los conectores SC en el Distribuidor Secundario (SDF) y Distribuidor Principal (MDF).
- Mangueras de 4 pares trenzados sin apantallar, categoría 5 ampliada, entre los Puntos de Entrada a la Red de Transmisión Activas y los Distribuidores Secundarios (SDFs).
- Paneles de montaje en rack de 19 pulgadas con 24 conectores RJ45 categoría 5E ampliada.
- Conectores RJ45 hembra categoría 5 ampliada en los Puntos de Entrada a la Red de Transmisión Activas. Estos módulos deben incorporar una tapa frontal guardapolvo, comandada por un muelle, tal que permanezca cerrada cuando no haya insertado un latiguillo.
- Conectores RJ45 macho de triple uña para conductor rígido, categoría 5E ampliada, para conexionado de latiguillos en cable rígido mediante herramienta de engastar conectores RJ45.
- Embarrado de tierra constituido por barras de 450x60x6mm con 80 tornillos de latón para distribución radial de tierras.

- Rail con 10 enchufes de energía eléctrica proveniente de SAI, comandados por un disyuntor magnetotérmico bipolar de 15ª

**Normas de instalación y etiquetado**

Todas las mangueras de cobre o fibra óptica, se tenderán en una sola pieza entre:

- Distribuidor Principal (MDF) y Distribuidor Secundario (SDF).
- Distribuidor Secundario (SDF) y Punto de Entrada a la Red de Transmisión Activa.

No se permite ningún tipo de empalme ni la instalación de ningún punto de transición.

Todos los conectores RJ45 irán numerados del 1 al n dentro de cada Distribuidor Secundario (SDF). Este valor se fijará tanto en el Punto de Entrada a la Red de Transmisión Activa como en el panel de los Distribuidores Secundarios (SDFs).

**Componentes activos, tecnología a usar y política de seguridad**

Con el fin de poner operativa la red de transmisión de datos sobre la red de cableado, es necesario usar electrónica de conmutación en los Distribuidores Secundarios (SDFs) y electrónica de conmutación y comunicación en el Distribuidor Principal (MDF).

Si bien las características del medio de transmisión (cables+conectores) que se instalarán en el edificio permitirían la conexión de equipos informáticos con interfases de conexión de propietario, en el presente proyecto, sólo se referirán aquellas interfases que son estándar y de dominio público, por tanto,

de forma explícita no se hará referencia a ninguna interfaz de propietario para soportar ningún tipo de servicio en relación con la red de comunicación de datos. Se asume que las técnicas de señalización mediante las que se conectarán los ordenadores y para las cuales se garantiza la interoperabilidad en el presente proyecto son:

- **IEEE 802.3 10Base-T** (Ethernet) a 10 Mbps para conexión de clientes, sobre cobre.
- **IEEE 802.3 10Base-FL** (Ethernet) a 10 Mbps para conexión de clientes con necesidad de aislamiento galvánico absoluto (equipos de instrumentación clínica), sobre fibra óptica.
- **IEEE 802.3 100Base-TX** (Fast Ethernet) a 100 Mbps para conexión de clientes o servidores sobre cobre.
- **IEEE 802.3 100Base-FX** (Fast Ethernet) a 100 Mbps para conexión de clientes con necesidad de aislamiento galvánico absoluto (equipos de instrumentación clínica), sobre fibra óptica.
- **IEEE 802.3z 1000Base-LX** (Gigabit Ethernet) a 1000 Mbps para conexión de servidores en la granja de servidores y estaciones que controlen equipos de producción de imágenes (PACS/IMACS), sobre fibra óptica

En la implementación de la intranet del hospital, de forma explícita no se considera la tecnología ATM (debido a su excesiva complejidad de gestión y configuración), ya que no hay ninguna aplicación relevante, que funcione en modo nativo ATM y que no se pueda implantar sobre tecnología Ethernet.

Siempre que haya comunicación visual entre el edificio del hospital y otros edificios en los que se alojen servicios clínicos que requieran comunicación con el mismo, se recomienda establecer conexiones punto a punto entre los edificios, usando redes inalámbricas de tecnología radio a 11 ó 20 Mbps, basadas en el estándar **IEEE 802.11**.

Para que la red de transmisión de datos sea capaz de absorber todo el tráfico sin congestión, la regla de oro a aplicar ("gold standard"), es que la relación entre el ancho de banda horizontal y vertical sea menor o igual a 4 (Meta Group, Nov 1998). Esto significa que por cada 4 canales activos (de una determinada velocidad **v**) de forma concurrente (4 ordenadores clientes generando tráfico de forma simultánea contra 4 servidores distintos) se debe disponer de un canal de velocidad **v,** que evacue dicho tráfico hacia los nodos con los que se establece el mismo. Si se asume un factor de simultaneidad del 16%, esto determina el ancho de banda necesario entre cada Distribuidor Secundario (SDF) y el Distribuidor Principal (MDF) en función del número de equipos conectados en cada Distribuidor Secundario (SDF), así como el ancho de banda mínimo necesario en la electrónica del Distribuidor Principal (MDF).

Este escenario plantea resolver por diseño las siguientes cuestiones:

- Que los clientes que la mayor parte de su tiempo, generen tráfico contra un determinado servidor, estén en la misma red que dicho servidor.
- Que al existir servidores distintos, que potencialmente van a ser accedidos concurrentemente en el tiempo por clientes distintos, se debe facilitar este paralelismo.

- Que el tráfico generado por la conversación de un cliente con un servidor no interfiera o paralice la conversación de otro cliente distinto con otro servidor distinto.
- Que cuando tenga que cursarse tráfico cruzado entre un cliente que está en una red y un servidor que está en otra, el cambiar de red se realice a la misma velocidad que si estuvieran en la misma.
- Que la función de contención de los datos, en el proceso de despacho de los mismos desde los servidores a los clientes, se desplace a la electrónica de transmisión para liberar a los servidores lo antes posible y que queden disponibles para nuevas peticiones.
- Que sólo se acceda a cada red desde máquinas autorizadas en función de su dirección.
- Que las tormentas de "broadcast" no degraden el funcionamiento de la red.
- Que la gestión de toda la red se realice desde un único punto.

Para que el comportamiento de la red del hospital sea eficiente, siendo eficaz la transmisión y la seguridad, (conceptos antagónicos, sino se diseñan de forma conjunta) se deben tomar ciertas decisiones sobre la forma en como se implantan los servicios de red. Esto quiere decir, que no se puede diseñar la implementación de los servicios sin tener presente de forma simultánea la política de seguridad. Algunas de estas decisiones son:

- NO realizar asignación dinámica de direcciones IP (identificadores de los ordenadores que se conectan a la red mediante protocolo DHCP) por razones de velocidad y seguridad.

- NO usar enrutamiento dinámico en la intranet del hospital por razones de seguridad y velocidad. En la primera parte del presente articulo ya se justificó porqué es absolutamente innecesario en la intranet del hospital instalar redundancia.
- NO usar direccionamiento privado para no perder tiempo en traducir direcciones privadas por direcciones legales en el proceso de conexión a internet a través de Telefónica del Perú SAA.
- NO usar ningún otro protocolo de red que no sea IP unicast o IP multicast, ya que es posible montar todos los servicios sobre este protocolo, además este protocolo permite hacer la puesta a punto en local de la parte cliente de las aplicaciones que van a funcionar de forma remota (desde ambulatorios, centros de salud, etc.). Particularmente se evitarán protocolos como el NetBios de Microsoft y todos los que trabajen en modo broadcast, por razones de rendimiento y seguridad.
- Incorporar en el router de conexión externa del hospital las siguientes reglas de seguridad al tráfico de entrada hacia el hospital, en el interfaz que le conecta con Internet:
    - Denegar el acceso de cualquier paquete proveniente de internet que contenga dirección IP origen, una dirección IP perteneciente a direccionamiento privado:

      Red 10.0.0.0 máscara 0.255.255.255

      Red 172.0.0.0 máscara 0.31.255.255

      Red 192.168.0.0 máscara 0.0.255.255
    - IP spoofing (denegar acceso a cualquier paquete proveniente de internet con dirección IP origen una

dirección IP perteneciente al espacio direccional del hospital.

- Denegar acceso a cualquier paquete proveniente de internet que pertenezca al servicio Net-BIOS.
- Denegar acceso a cualquier paquete proveniente de internet con destino cualquier servidor interno del hospital (que aloje información sensible).
- Permitir el paso de paquetes SMTP (correo electrónico) provenientes de internet si y sólo si, van con dirección IP destino, el servidor de correo electrónico oficial del hospital.
- Permitir el paso de paquetes web provenientes de internet si y sólo si, van con dirección IP destino, al servidor web oficial del hospital.
- Permitir el paso de paquetes provenientes de internet sólo si son paquetes respuesta a sesiones iniciadas previamente desde dentro el hospital (el servicio ftp tiene tratamiento específico).
- Permitir el paso de paquetes de solicitudes de DNS provenientes de internet si y sólo si, van con dirección IP destino, el servidor DNS oficial del hospital.
- Permitir el paso de paquetes ICMP provenientes de internet si y sólo si, van con dirección IP destino a: router de acceso, servidor oficial DNS, servidor oficial correo

electrónico, servidor oficial ftp anónimo y servidor oficial web.

- Permitir el paso de paquetes NTP provenientes del servicio de tiempo de Telefónica del Perú SAA hasta el router de acceso, que actuará como servidor de tiempo del hospital.
- Denegar el acceso a cualquier otro paquete que no se haya permitido pasar en las reglas previas.

- IncoDistribuidor Principal (MDF)orar en el router de conexión externa del hospital las siguientes reglas de seguridad al tráfico de salida del hospital, en el interfaz que le conecta con Internet (RedIRIS):
    - IP smoorfing (denegar la salida a cualquier paquete proveniente del hospital con direccion IP origen una direccion IP que no pertenece al espacio direccional del hospital.

**Arquitectura de la Solución**

La solución que se propone estará basada en una red de área local con el siguiente equipamiento en el Distribuidor Principal (MDF) y Distribuidores Secundarios (SDFs):

- En el Distribuidor Principal (MDF), un router para acceso externo del hospital. En este equipo se conectarán todas las líneas que a través de operadores públicos de comunicaciones, comunican el hospital con los centros de salud de su área sanitaria, centros directivos, etc. Típicamente este router dispondrá de interfases serie síncronas o RDSI acceso básico para conexión con los centros de salud, interfaz serie

síncrona para conexión con Telefónica del Perú y 2 interfases LAN, una para la conexión de la red no protegida o desmilitarizada, que aloja todos los servidores públicos del hospital (correo, DNS, ftp, web que pueden estar sobre la misma máquina) y en el otro interfaz, para la conexión de la red protegida o militarizada (intranet del hospital). Este interfaz conecta con el conmutador central del hospital.

- En el Distribuidor Principal (MDF) un conmutador de nivel 3 (router+conmutador de tramas LAN integrados en el mismo bus) a velocidad de cable que conecta las diferentes redes virtuales LAN (sobre las que se superponen redes IP de máscara variable). A este conmutador se conectan los conmutadores de nivel 2 de los Distribuidores secundarios (SDFs) y todos los servidores.
- En los Distribuidores Secundarios (SDFs) conmutadores de nivel 2 (conmutadores de tramas LAN) a los que se conectan a 10 o 100Mbps los equipos finales.

Es conveniente que el conmutador del Distribuidor Principal (MDF) incorpore 2 fuentes de alimentación conectadas a 2 circuitos eléctricos distintos provenientes del SAI y gestionados por 2 dispositivos diferenciales distintos.

A continuación se ilustra el esquema de conexión de la red de datos del Hospital de Apoyo JAMO.

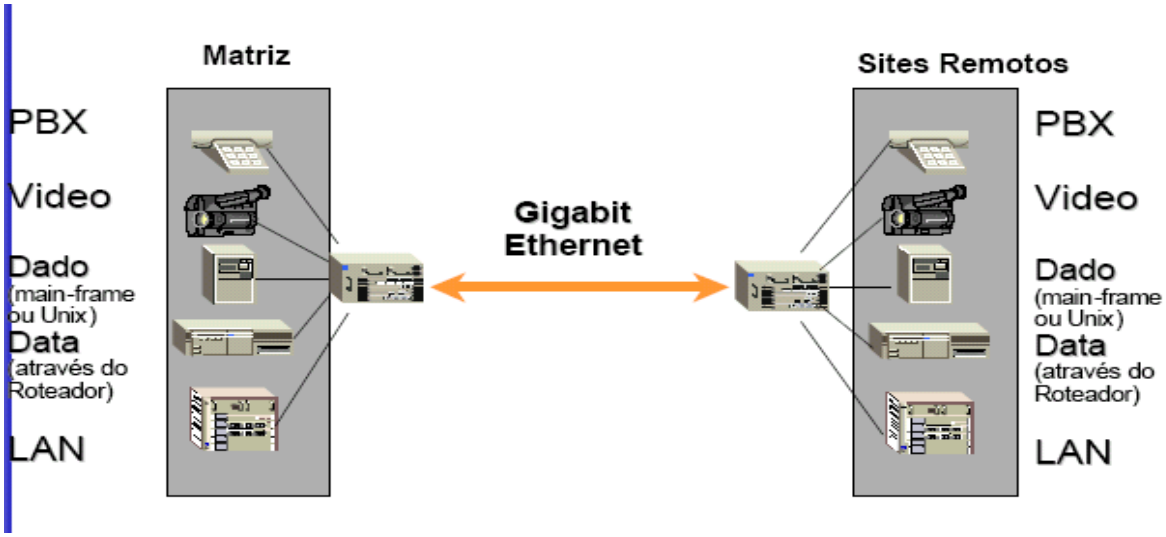



*Figura Nº 57  Esquema la arquitectura de Soluciones (Backbone)*

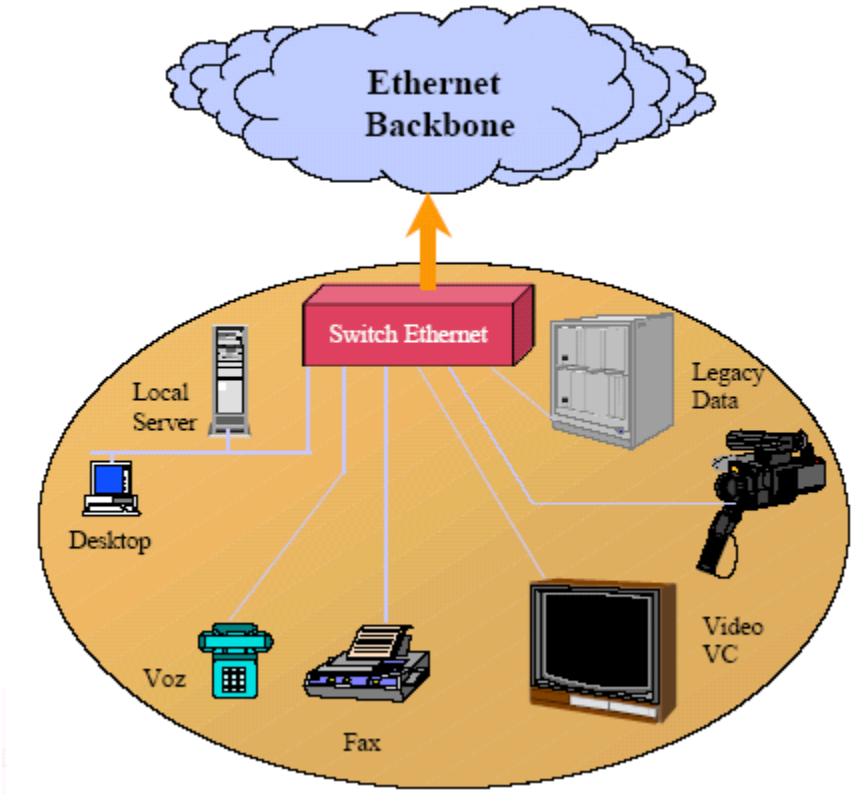



*Figura Nº 58  Esquema de Soluciones Integrales*

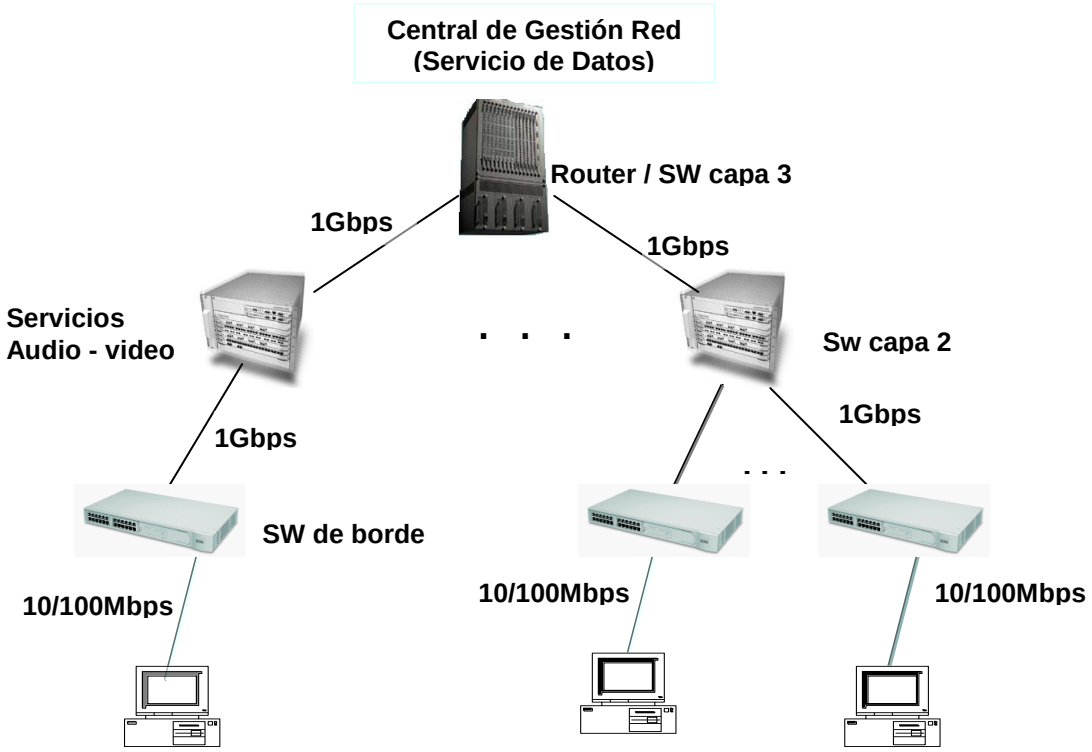



***Figura Nº 59  Esquema la Distribución de la Red de Datos del Hospital***

# CAPITULO VI

# COSTOS DEL PROYECTO

El costo económico de interconectividad se presentará de manera estándar, presentando al final un presupuesto global que demanda instalar una Red de Comunicaciones en el Hospital de Apoyo JAMO.

## 6.1. Cotización de Equipos de Red

En cuanto a los equipos de conmutación que se usarán en la red de comunicaciones a continuación se presenta una cotización global de la inversión.

***Tabla Nº 04 Equipos de Conmutación***

| **Central de Gestión Red (CGR) - Servicios Administrativos Hospitalarios** | | | | |
|---|---|---|---|---|
| **PN** | **Descripción** | **Cantidad** | **Precio Unitario ($)** | **Precio Total ($)** |
| 3CRWE754672 | 3COM Internet Gateway Routers Office Connect ADSL Wireless 11g Firewall Router | 1 | 241.99 | 241.99 |
| 3C1770110 | 3COM Super Stack 3 Switch 4924 24 Ports 100/1000 Base Tx | 1 | 4547.99 | 4547.94 |
| 3C17203 | 3COM Super Stack 3 Switch 4400 Family 24 Ports | 2 | 1459.99 | 2919.98 |

| | |
|---|---|
| **Sub-Total** | 7709.91 |
| **I.G.V.** | 1464.88 |
| **TOTAL** | 9174.79 |

***Tabla Nº 05  Equipos para el Cuarto de Telecomunicaciones***

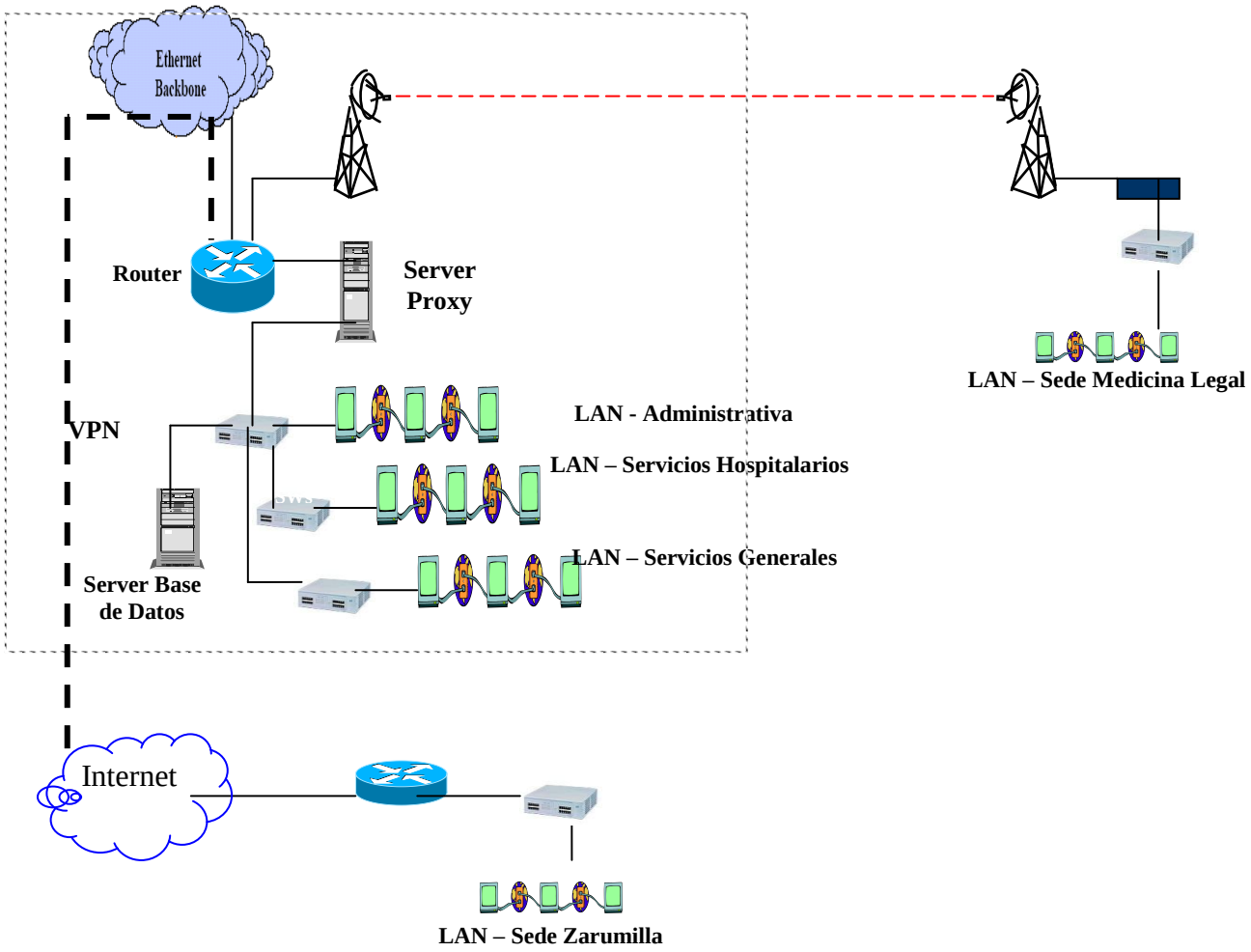
| EQUIPO | **DESCRIPCIÓN** | **MARCA / CODIGO** | **CANTIDAD** | **COSTO POR UNIDAD** | **TOTAL (Incluye IGV) $** |
|---|---|---|---|---|---|
| Rack. | RS2 Rack System. | SIEMON / RS2-07 | 1 | 121.99 | 121.99 |
| Patch Pannel. | Ultra HD6 Patch Pannel / 48 ports. | AMP / 1375015-1 | 2 | 359.38 | 718.76 |
| Ordenador Horizontal. | Horizontal Finger Duct Panels, Single-Sided. | AMP / 1375161-1 | 5 | 31.5 | 157.5 |
| Ordenador Vertical. | Vertical Finger Duct Panels, Single-Sided | AMP / 1375165-1 | 2 | 58.9 | 117.8 |
| **TOTAL** | | | | | **1116.05** |

***Tabla Nº 06 Accesorios para el Cableado Estructurado***

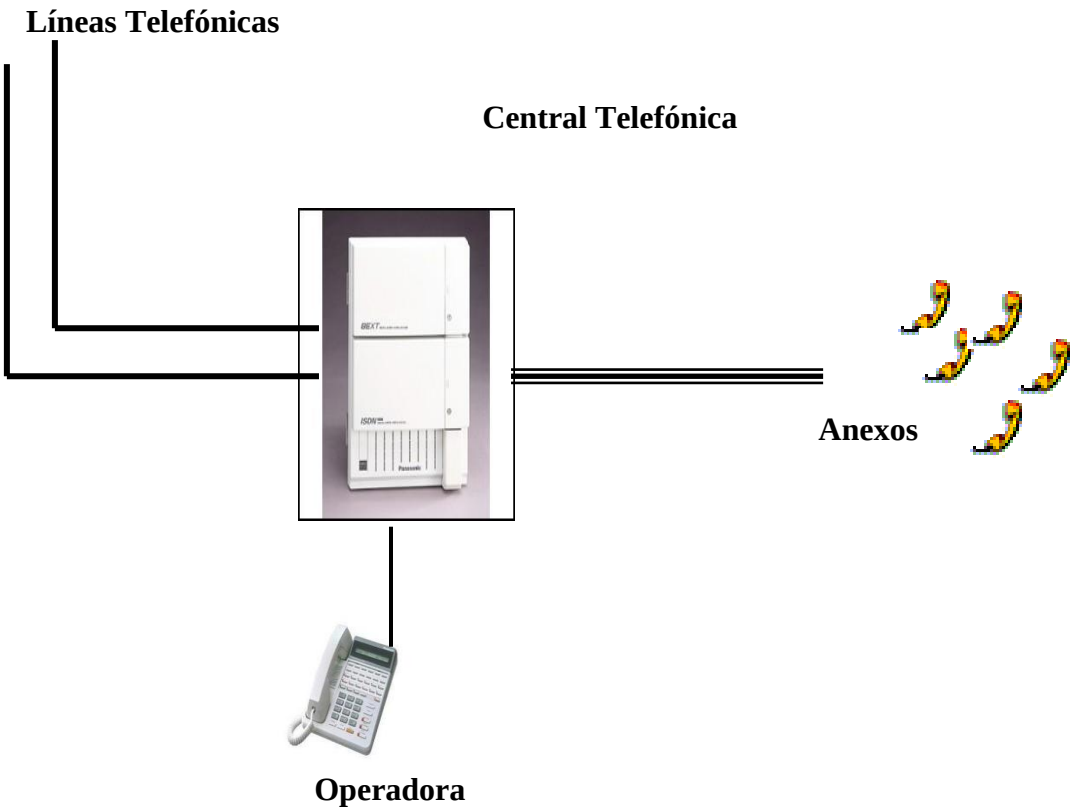
| Accesorios para el cableado | Descripción | Marca/Código | Total Aprox. | | Costo por Unidad | Total |
|---|---|---|---|---|---|---|
| **Cable UTP.** | Categoría 6UTP | AMP /219567-5 | 2998.87 m. | Aprox. 10 rollos | 135.99 | 1359.9 |
| **Patch Cord UTP.** | MC6 Modular Cords | SIEMON / MC6-8-T-10-06 | | 64 patch cords. | 12.99 | 831.36 |
| **Couplers** | Angled CT6 Couplers. | SIEMON / CT-C6-C6-02 | | 64 couplers | 11.99 | 767.36 |
| **Faceplate** | Stainless Stell CT Faceplates | SIEMON / CT4-FP-SS | | 64 faceplates | 1.89 | 120.96 |
| **Canaletas** | **Derivación T** | | | | | |
| | de 10 cables. | Hellermann /CT2734 27x30 | 10 | Tipo T. | 0.55 | 5.5 |
| | de 6 cables. | Hellermann /AT1825 18x21 | 60 | Tipo T. | 0.35 | 21 |
| | de 2 cables. | Hellermann /AT151 14x7 | 10 | Tipo T. | 0.2 | 2 |
| | **Ángulos 90º** | | | | | |
| | de 10 cables. | Hellermann /CP2735 27x30 | 15 | 15 codos. | 0.55 | 8.25 |
| | de 6 cables. | Hellermann /AR1824 18x21 | 80 | 80 codos. | 1.3 | 104 |
| | de 2 cables. | Hellermann /AR150 14x7 | 20 | 20 codos. | 0.2 | 4 |
| | **Standar** | | | | | |
| | de 10 cables. | Hellermann /FSR27305 27x30 | | 1800.35 m. | 3.10 (Pzx2m) | 2790.54 |
| | de 6 cables. | Hellermann /F1821 18x21 | | 859.25 m. | 1.30 (Pzx2m) | 558.51 |
| | de 2 cables. | Hellermann /F147 14x7 | | 339.27 m. | 0.62 (Pzx2m) | 105.17 |
| Tarjeta de Red | NIC 10/100 | D-Link / DFE-550TX | 10 | 10 NIC's | 28 | 280 |
| **TOTAL** | | | | | | **6958.55** |
| **IGV** | | | | | | **1322.12** |
| **TOTAL** | | | | | | **8280.67** |

Los equipos de conmutación se presentan en distintos modos y empresas que distribuyen una gran variedad de los mismos.

***Propuesta de la Red de Comunicación de Datos***



***Propuesta de una Central Telefónica (Red de Telefonía)***

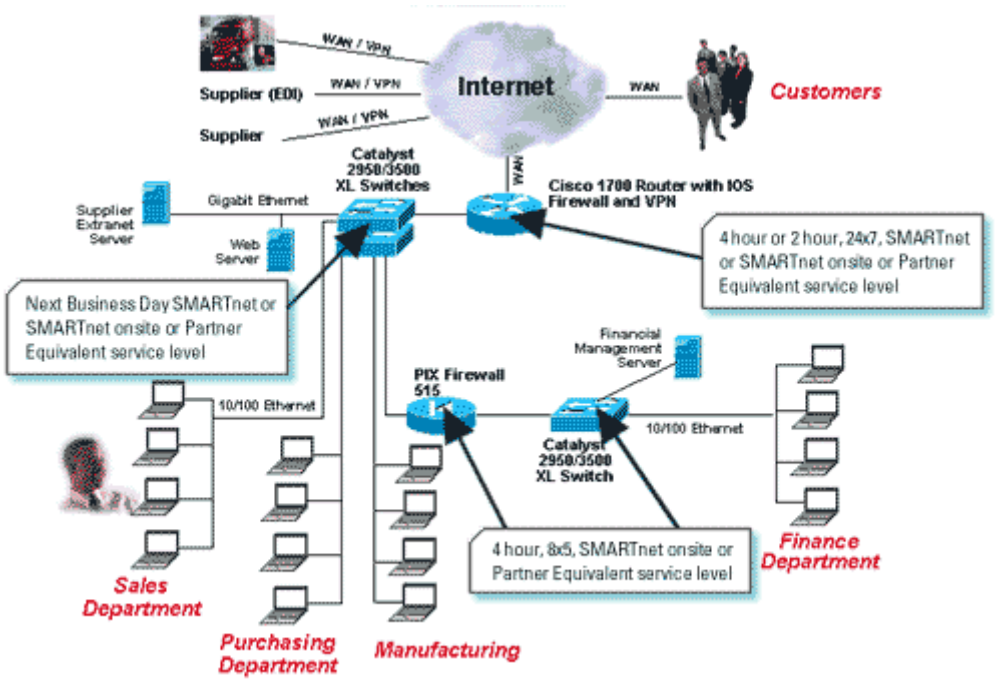



El presente presupuesto, se tomo en consideración al estudio de costos de equipos y materiales en el mercado actual, para el desarrollo básico del proyecto. (Ver Anexos)

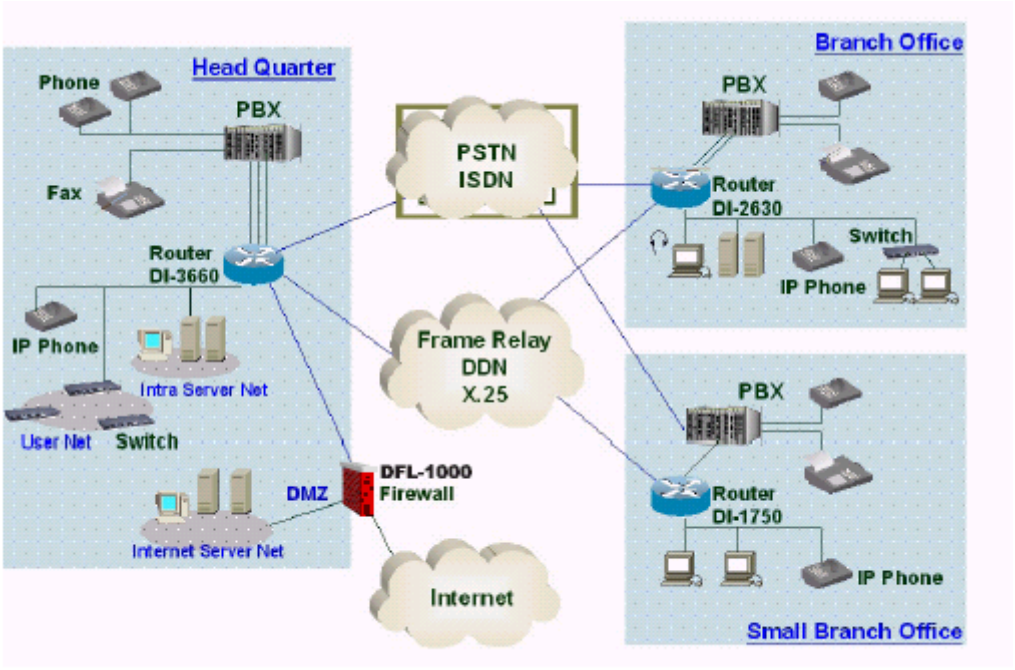
Se eligió los equipos generalmente de la marca 3COM, debido a una evaluación técnica (confiabilidad, flexibilidad a los cambios, homogeneidad, velocidad, y calidad de servicio) y de costo-beneficio. (Ver Anexos)

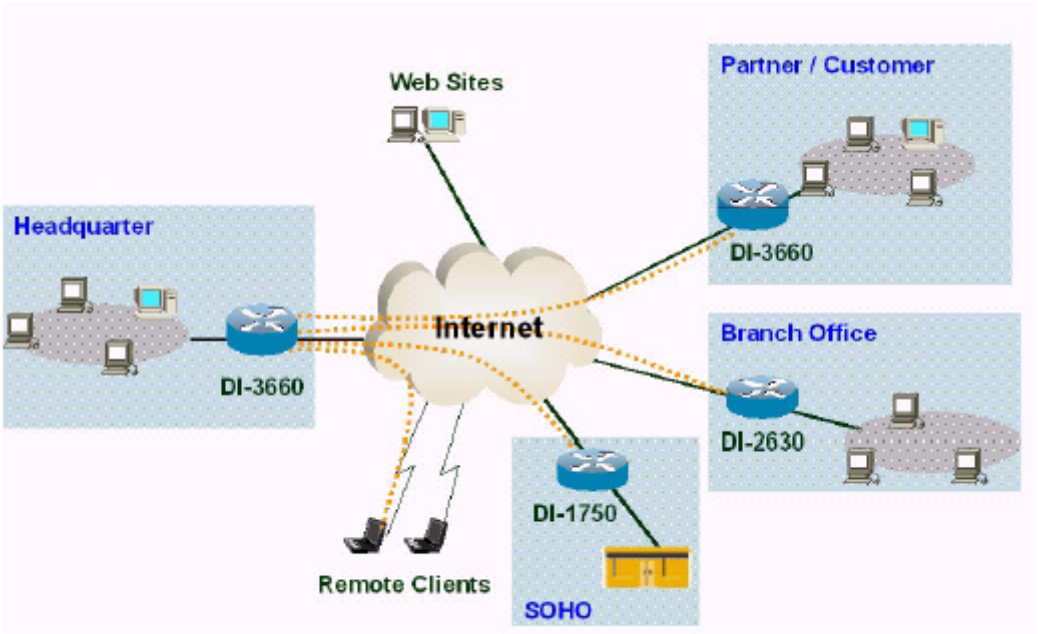
## 6.2. Propuestas de Diseño y Aplicaciones (Empresas)

***CISCO***

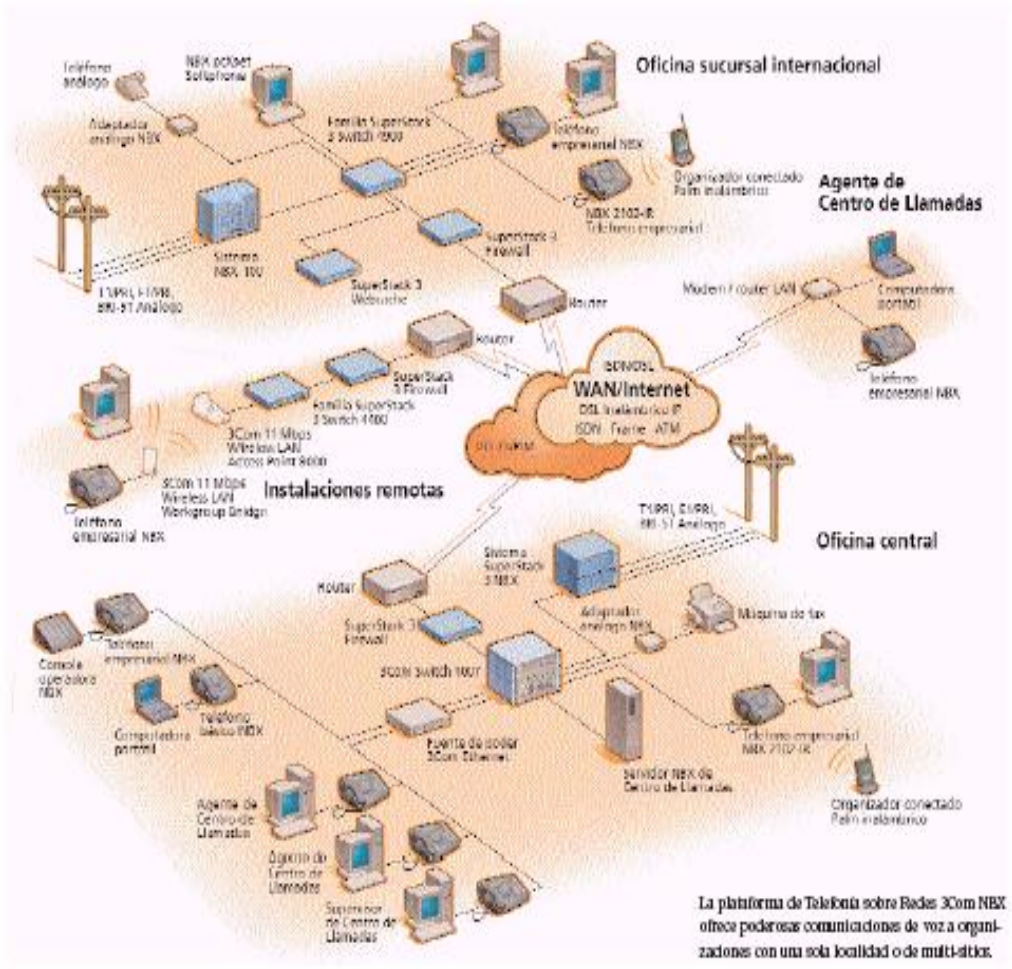


***DLink***


Head Quarter
Phone
PBX
Fax
Router
DI-3660
IP Phone
Intra Server Net
User Net
Switch
DMZ
DFL-1000
Firewall
Internet Server Net
PSTN
ISDN
Frame Relay
DDN
X.25
Internet
Branch Office
PBX
Router
DI-2630
Switch
IP Phone
PBX
Router
DI-1750
IP Phone
Small Branch Office


Web Sites
Partner / Customer
DI-3660
Headquarter
DI-3660
Internet
Branch Office
DI-2630
DI-1750
Remote Clients
SOHO

**3COM**




La plataforma de Telefonía sobre Redes 3Com NBX ofrece poderosas comunicaciones de voz a organizaciones con una sola localidad o de multi-sitios.

## IV. CONCLUSIONES, RECOMENDACIONES Y PERPESTIVAS

- El Hospital de Apoyo “JAMO” – Tumbes, no cuenta con una red de comunicaciones que brinde los servicios de voz, datos y video.
- Existe redes individuales por servicios las cuales no tienen el servicio de Internet.
- El cableado de cada red individual no cumple con los estándares normalizados.
- Habiendo realizado el Estudio de Diseño y Económico se propone la tecnología Ethernet, la interconexión entre los distintos servicios administrativos – hospitalarios.
- El punto de enlace del Servicio de Internet se centrara en un Centro de Telecomunicaciones.
- Se requiere la adquisición de nuevos equipos de red para lograr un servicio eficiente.
- El tendido del Cableado Estructurado se desarrollara mediante Cable UTP Categoría 5E o 6, mediante canalización y aéreo.
- En la actualidad en el avance tecnológico medico-hospitalario, así como brindar un servicio de calidad a los pacientes, haciendo más rápida y eficiente el sistema de comunicaciones dentro de la institución, por lo cual el servicio de enlace de internet debe realizarse lo más pronto posible.

## V. REFERENCIAS BIBILIOGRAFICAS Y WEB SITES


[1] GRALLA, P.: **"Como Funcionan las Intranets"**, 1ra ed. Maylands: Prentice Hall. 1996.

[2] CABALLERO, José Manuel.: **"Redes de Banda Ancha"**, Editora Alfa Omega.

[3] **Desarrollo y Aplicaciones.** Disponible en: http://vobo.com.mx/intranet.html 1999.

[4] Catálogo **"AMP NetConnect"**, 2003.

[5] Soluciones Cisco, **"Migrating to an IP Telephony Network"**, 2003 http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns268/networking_solutions_package.html

[6] GARCÍA Tomás Jesús; FERRANDO, Santiago; PIATTINI, Mario.: **"Redes para Proceso Distribuido"**, Editora Alfa Omega, 1º Edición, México,1997.

[7] Guía del **"Curso de Especialización y Conectividad en Redes"**, Escuela Tecnológica- Universidad de Piura, 2003.

[8] Guía del **"Curso de Cableado Estructurado"**, INICTEL, Lima, 2002

[9] **Intranet**, en http://www.wntmag.com/atrasados/1996/02_oct96/intranet.html

[10] TANEMBAUN, Andrew S.: **"Redes de Computadoras"**, Prentice Hall, Tercera Edición, 1997.

[11] **Redes de Comunicaciones en Salud:** www.rediris.es/rediris/boletin/66-67/ponencia3.pdf

[12] Guía Teoría – Practica Certificación CCNA – CISCO, ETS – UDEP 2003

## Glosario de Términos

| | |
|---|---|
| A.R.P.A.N.E.T. | Advanced Research Projects Agency. Progenitora de Internet, fue A.R.P.A.N.E.T., perteneciente al departamento de defensa de los Estados Unidos. Desarrollado como herramienta de uso militar y de investigación. |
| ADSL | Abreviación de Asymmetric Digital Subscriber Line. ADSL es un método de transmisión de datos a alta velocidad a través de las líneas telefónicas de cobre tradicionales. Es asincrónica, ya que el ancho de banda asignado para downstream es mucho mayor que el ancho de banda de upstream. Esta tecnología es adecuada para el web, ya que es mucho mayor la cantidad de datos que se envían desde el servidor a un computador personal que desde un computador personal a un servidor. |
| ALWAYS ON | Siempre conectado. Servicio de acceso a Internet que se caracteriza por brindar las 24 horas del día servicio de acceso a Internet. Este servicio ha sido impuesto por conexiones de banda ancha que a través de un único pago mensual, permite a sus clientes conectarse a Internet, sin restricciones de horario ni tiempo que dure la conexión. |
| ANCHO DE BANDA | Es la capacidad para transportar datos que posee un medio en particular. Normalmente se mide en Megabites por segundo (Mb/s) o en Gigabites por segundo (Gb/s). Un ejemplo de esto sería una manguera de jardín que transporta una cantidad determinada de litros de agua por segundo, pero cuanto mayor sea el diámetro de la manguera, más agua transportará. El ancho de banda se mide en Hertz ("ciclos por segundo") o en bits por segundo (bps), por eso, es uno de los factores más importantes que determinan la velocidad de la conexión a Internet. |

| | |
|---|---|
| ATM | Modo de Transferencia Asincrónica. La tecnología llamada Asynchronous Transfer Mode (ATM) es el corazón de los servicios digitales integrados que ofrecen las nuevas redes digitales de servicios integrados de Banda Ancha. El tráfico del ciberespacio, con su voluminoso y tumultuoso crecimiento, impone a los operadores de redes públicas y privadas una alta demanda de ancho de banda y flexibilidad de soluciones robustas. La versatilidad de la conmutación de paquetes de longitud fija, denominadas celdas ATM, son las tablas más calificadas para soportar la demanda de Internet. Cada celda compuesta por 53 bytes, de los cuales 48 (opcionalmente 44) son para transporte de información y los restantes para uso de campos de control. |
| BACKONE | Un backbone es el enlace de gran caudal o una serie de nodos de conexión que forman un eje de conexión principal. Es la columna vertebral de una red. Por ejemplo, NSFNET fue el backbone, la columna o el eje principal de Internet durante muchos años. |
| BIT | Abreviación de binary digit, un bit es la unidad más pequeña de datos que un ordenador puede manejar. Los bits se utilizan en distintas combinaciones para representar distintos tipos de datos. Cada bit tiene un valor 0 ó 1. |
| BPS | Es la abreviación de bits per second (bits por segundo). BPS es una medida de velocidad, que registra el número de bits que son transmitidos en un segundo. Es utilizado para medir la velocidad de un módem o la velocidad de una conexión digital. |
| BYTE | Serie de 8 bits. Un Byte puede representar una letra, un número, un símbolo. |

| | |
|---|---|
| CABLE COAXIAL | Es el tipo de cable usado por las compañías de televisión por cable para establecer la conexión entre la central emisora y el usuario. También se lo utiliza en las conexiones de redes de área local (L.A.N.). El cable coaxial esta conformado por un núcleo de cobre, aislado por plástico de un recubrimiento metálico y este a su vez envuelto en otra capa de plástico. Suelen emplearse dos tipos de cable coaxial para las redes locales: cable de 50 Ohms, para señales digitales, y cable de 75 Ohms, para señales analógicas y para señales de alta velocidad. |
| CABLE MÓDEM | Tecnología, que permite acceso a Internet a través de las redes de televisión por cable. Las velocidades de conexión ofrecidas en el mercado oscilan entre los 64 y 960 Kbps. |
| CARRIER | Portadora. Carrier es una señal o pulso transmitido a través de una línea de telecomunicación. Un carrier es también una empresa que opera en el sector de las telecomunicaciones ofreciendo servicios de telefonía de larga distancia e internacional. |
| CEBIT | Feria de informática más grande de Europa. Se celebra en la ciudad alemana de Hannover. Suele atraer a las más importantes empresas del sector y a un gran número de visitantes. Se celebra anualmente en el mes de marzo. |
| CERN | Laboratorio europeo de física de partículas. Fue el desarrollador inical del World Wide Web. Actualmente los estándares del Web son desarrollados por la World Wide Web Organization (3WO). |
| CONEXIÓN POR MÓDEM | Es una forma de conexión a Internet a través de las líneas telefónicas. A través de un proveedor de Internet (ISP), la cuenta permite usar un módem para establecer una conexión con el sistema del proveedor. Una vez que se ha marcado el número del proveedor y estando |

| | |
|---|---|
| | conectado, el proveedor conecta al usuario a Internet. Se pueden visitar sitios web por medio de un navegador. Existen distintos tipos de cuenta de conexión por módem. Las cuentas SLIP o PPP permiten navegar en el World Wide Web directamente a partir del sistema operativo Windows o Macintosh. |
| CHAT | Charla. Servicio de Internet que permite a dos o más usuarios conversar en tiempo real mediante el teclado. |
| DIRECCIÓN DE CORREO ELECTRÓNICO | Se refiere a la dirección de correo de un ordenador a la cual se pueden enviar mensajes electrónicos. Cada sistema de ordenadores maneja de manera distinta la dirección del correo, pero se basa en varios protocolos para intercambiar correo con otros sistemas diferentes. |
| DIRECCIÓN IP | La dirección del protocolo de Internet (IP) es la dirección numérica de una computadora en Internet. Cada dirección electrónica se asigna a una computadora conectada a Internet y por lo tanto es única. La dirección IP esta compuesta de cuatro octetos de bits. Un octeto se refiere a ocho bits que conforman un byte. |
| DMT | Multi Tono Discreto. Técnica de transmisión de datos que divide un canal en cientos de subcanales. Cada subcanal es testeado para determinar el nivel de ruido existe. Una vez concluida la revisión, el sistema enviará más o menos bits por cada canal, dependiendo el nivel de interferencia que presente cada uno. |
| DNS | Sistema de nomenclatura de dominios (Domain Name System) Es un sistema que se establece en un servidor (que se encarga de un dominio) que traduce nombres de computadores (www.servidor.dgsca.unam.mx) a domicilios numéricos de Internet (132.248.10.1). |

| | |
|---|---|
| DOMÓTICA | Tecnología basada en el uso del protocolo de comunicación X10, el cual permite controlar y automatizar electrodomésticos tradicionales (televisores, lavadoras, microondas) y otros artefactos eléctricos (portones, luces, riego de jardín) a distancia. |
| DOWNLOAD | Descargar, bajar. Transferencia de información (archivos) desde Internet a un computador. |
| DOWNSTREAM | Flujo de datos que es recibido por un computador. El flujo de datos es medido en bps. |
| E1 | Consta de 32 canales de 64 Kbps, 30 canales para transmitir voz y 2 canales para transmitir información de sincronismo y señalización de línea. |
| EMAIL | Abreviación de electronic mail. Consiste en mensajes de texto enviados de un usuario a otro por medio de una red. |
| ETHERNET | Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus, anillo, estrella. La red ethernet ofrece un ancho de banda de 10 y 100 Mbps siendo éstas las velocidades más populares. |
| FCC | Federal Communications Commission. Entidad encargada de regular los límites de exposición humana a las ondas de radio frecuencia. |
| FRECUENCIA | Número de ciclos o periodos completos de corriente producidos por un generador de corriente alterna por segundo. La unidad de frecuencia llamada ciclo por segundo, hoy es llamada hertzio. Cuando una frecuencia supera los 10.000 ciclos, es llamada alta frecuencia, cuando es inferior a este número, es llamada baja frecuencia. |
| FULL DUPLEX | Característica de una comunicación que permite transmitir información |

| | |
|---|---|
| | al mismo tiempo que la recibe, de manera similar a un teléfono convencional. |
| GATEWAY | Puente. Sistema de información que transfiere información entre sistemas o redes incompatibles. |
| GIGA | Prefijo que indica un múltiplo de 1.000 millones, o sea $10^9$. Cuando se emplea el sistema binario, como ocurre en informática, significa un múltiplo de $2^{30}$, es decir 1.073.741.824. |
| GIGABIT | Aproximadamente 1.000 millones de bits (exactamente 8.589.934.592 bits). |
| GIGABYTE | Unidad de medida. 1 giga byte es equivalente a 1.073.741.824 bytes. |
| HALF DUPLEX | Transmisión de información bidireccional sobre un medio común, por donde la información sólo puede viajar en una sola dirección en un tiempo. Esto permite transmitir o recibir información. |
| HERTZ | Hercio, unidad de frecuencia electromagnética. Equivale a un ciclo por segundo. |
| HFC | Hybrid Fiber Coaxial. Red híbrida que está compuesta por tramos de fibra óptica y tramos de cable coaxial. |
| HIPERTEXTO | Hipertexto se refiere a cualquier texto disponible en el World Wide Web que contenga enlaces con otros documentos. Utilizar el hipertexto es una manera de presentar información en la cual texto, sonido, imágenes y acciones están enlazadas entre sí de manera que se pueda pasar de una a otra en el orden que se desee. |
| HTML | Siglas de Hypertext Markup Language. El HTML es el lenguaje informático utilizado para crear documentos hipertexto. El HTML utiliza una lista finita de rótulos o tags, que describe la estructura general de |

varios tipos de documentos enlazados entre sí en el World Wide Web.

HTTP — HTTP son las siglas de HyperText Transfer Protocol, el método utilizado para transferir ficheros hipertexto por Internet. En el World Wide Web, las páginas escritas en HTML utilizan el hipertexto para enlazar con otros documentos. Al pulsar en un hipertexto, se salta a otra página web, fichero de sonido, o imagen. La transferencia hipertexto es simplemente la transferencia de ficheros hipertexto de un computador a otro. El protocolo de transferencia hipertexto es el conjunto de reglas utilizadas por los ordenadores para transferir ficheros hipertexto, páginas web, por Internet.

INDOOR — Es toda la estructura de la red eléctrica que se encuentra al interior de una vivienda, desde la puerta hacia adentro.

INTERNET — Internet fue un proyecto del Ministerio de Defensa estadounidense conocido como A.R.PA.N.E.T. Tras haber transcurrido algunos años, el Reino Unido se integró a la red que cubría a gran parte de las universidades y centros científicos de Estados unidos. Con el paso del tiempo se conectarían los demás países de Europa y algunos países de Asia. En los noventa ya se hablaba de una red internacional. Pero fue hasta la aparición de WWW que se logró conectar a millones de personas desde sus hogares y lugares de trabajo para unificar los recursos, esto trajo consigo el comercio, los negocios financieros, y el entretenimiento. Internet es una colección de miles de redes de ordenadores, es por ello que constituye un fenómeno sociocultural y comunicacional de gran escala, una nueva forma de realizar comunicaciones. Millones de personas acceden a la mayor fuente de información, la cual permite que ésta fluya en ambos sentidos. Internet

es una herramienta de trabajo, un periódico global, un buzón de correos, una tienda de software, una biblioteca, una plaza pública, un recurso educativo, una plataforma publicitaria. Cuatro características podrían definir las virtudes de Internet:

1. Grande, la mayor red de ordenadores del mundo;
2. Cambiante, se adapta continuamente a las nuevas necesidades y circunstancias;
3. Diversa, da cabida a todo tipo de equipos, fabricantes, redes, tecnologías, medios físicos de transmisión, usuarios, y
4. Descentralizada, no existe un controlador oficial, está controlada por los miles de administradores de pequeñas redes que hay en todo el mundo.

ISDN/RDSI — Siglas de Integrated Services Digital Network. Las líneas ISDN son conexiones realizadas por medio de líneas telefónicas ordinarias para transmitir señales digitales en lugar de analógicas, permitiendo que los datos sean transmitidos más rápidamente que con un módem tradicional.

ISP — Siglas de Internet Servie Provider. Hace referencia al sistema informático remoto al cual se conecta un computador personal y a través del cual se accede a Internet.

KILOBIT — 8192 bits.

KILOBYTE — 1024 bytes.

L.A.N. — Local Area Network. Red de área local. Conjunto de computadores interconectados a través de un medio físico (a través de cable UTP o cable coaxial), los cuales se encuentran en una misma área geográfica. Una L.A.N. permite compartir recursos, archivos, información, optimizando el uso de ellos.

M.A.C. — En una red los terminales comparten un único medio de transmisión.

| | |
|---|---|
| | Esto provoca que sea necesario establecer un protocolo para asegurar que el medio de transmisión sea utilizado de forma racional y equitativa. El protocolo de Control de Acceso al Medio (M.A.C.) distribuye los recursos del medio de transmisión para los usuarios que lo utilizan. |
| M.A.N. | Red de Área Metropolitana. Red que no supera los 100 kilómetros de cobertura. Computadores y equipos periféricos conectados en una ciudad o en varias ciudades conforman una M.A.N. |
| MB | Mega byte |
| Mb | Mega bit |
| MEGA BYTE (MB) | Unidad de medida. 1 mega byte es equivalente a 1.048.576 bytes. |
| MEGAHERTZ (MHz) | Un millón de hertz o hercios. |
| MÓDEM ANÁLOGO | Aparato que conecta dos o más computadores a través de una línea telefónica. Actúa trasformando las señales digitales del computador (bits) en tonos que son transmitidos por la línea telefónica. Igualmente, recibe los tonos que vienen por la línea telefónica y los convierte en señales digitales. Su nombre viene de la abreviación de las palabras modulador - demodulador. |
| MÓDEM PLC | Su función es introducir la señal digital en el cable de electricidad para que ésta viaje a través de el. También debe separar las señales de información de la señal eléctrica para que éstas ingresen al computador. |
| NSFNET | National Science Foundation's NETwork. La NSFNET comenzó con una serie de redes dedicadas a la comunicación de la investigación y de la educación. Fue creada por el gobierno de los Estados Unidos, y fue reemplazada por A.R.P.A.N.E.T. como backbone de Internet. Desde |

| | |
|---|---|
| | entonces ha sido reemplazada por las redes comerciales. |
| NT1 | Terminación de red 1. Localizado al interior de una vivienda de un abonado, es el responsable de ejecutar funciones de bajo nivel en una sistema de telefonía ISDN. |
| NT2 | Equipo multiplexor que permite tener conectado varios equipos terminales a un mismo terminal NT1. |
| OUTDOOR | Es toda la instalación eléctrica que se encuentra desde la puerta de la vivienda hacia el exterior, esto incluye las líneas eléctricas desde el medidor hacia el poste de energía eléctrica, el transformador de energía, las redes de baja, media y alta tensión. |
| P2P | Peer to Peer. Programas de intercambio de archivos entre usuarios de Internet. |
| PÁGINA WEB | Una página web es un documento creado en formato HTML (Hypertext Markup Language) que es parte de un grupo de documentos hipertexto o recursos disponibles en el World Wide Web. Una serie de páginas web componen lo que se llama un sitio web. Los documentos HTML, que estén en Internet o en el disco duro del ordenador, pueden ser leídos con un navegador. Los navegadores leen documentos HTML y los visualizan en presentaciones formateadas, con imágenes, sonido, y video en la pantalla de un computador. Las páginas web pueden contener enlaces de hipertexto con otros lugares dentro del mismo documento, o con otro documento en el mismo sitio web, o con documentos de otros sitios web. También pueden contener formularios para ser llenados, fotos, imágenes interactivas, sonidos, y videos que pueden ser descargados. |
| PC | Personal Computer. Se refiere a todos los computadores personales |

| | |
|---|---|
| | basados en la arquitectura del Personal Computer IBM presentado en 1981. El PC fue una máquina basada en un microprocesador Intel 8088. |
| PCMCIA | Personal Computer Memory Card International Asociation. Tarjetas de expansión que encajan en pequeñas ranuras, las cuales permiten aumentar las capacidades de computadores portátiles. |
| PLC | Powerline Communications. |
| POWERLINE COMMUNICATIONS | PLC es una tecnología que utiliza los tendidos eléctricos de media y baja tensión de una ciudad como canales de comunicación para transmitir señales digitales de voz y datos. Las velocidades que se pueden logran pueden variar entre 1 y 12 Mbps. La gran ventaja de un red PLC es la capacidad de convertir el cableado eléctrico de un hogar en una red de alta velocidad, convirtiendo cada enchufe disponible, en un potencial punto de conexión a Internet. |
| POWERNET | Nombre con el cual es comercializado en Alemania la tecnología Powerline Comunnications. |
| PPP | Siglas de Point-to-Point Protocol. Es un protocolo de comunicaciones utilizado para transmitir datos de la red a través de las líneas telefónicas. PPP permite comunicación directamente entre computadores de la red por medio de conexiones TCP/IP. |
| PROTOCOLO | Un protocolo es una serie de reglas que utilizan dos computadores para comunicar entre si. |
| PROTOCOLO DE COMUNICACIÓN | Conjunto de normas que definen cómo se realiza el intercambio de datos entre computadores o programas computacionales, organizando |

| | |
|---|---|
| | el desplazamiento de la información a través de la red e indicando cuál es el origen de los datos, el camino que deben recorrer y el destino final, es decir, es como un lenguaje adoptado convencionalmente entre los usuarios de una red para que puedan comunicarse y entenderse entre ellos. |
| PSTN | Servicio de Red de Telefonía Pública. |
| R2 | Protocolo utilizado en redes de telefonía del tipo E1. |
| RED | Es un conjunto de computadores (dos o más) que están unidos entre sí a través de elementos de comunicaciones, que pueden ser permanentes (como cables) o bien temporales, como enlaces telefónicos u otros. Dependiendo de su tamaño, las redes se clasifican en L.A.N. (Local Area Network), M.A.N. (Metropolitan Area Network) y W.A.N. (Wide Area Network). |
| RED ENLACES | En el contexto de la Reforma Educacional chilena, el Ministerio de Educación inició en 1992 el programa de informática educativa, conocido como Red Enlaces. Enlaces tiene la mirada dirigida hacia el futuro, en el que se espera que estudiantes y profesores logren la aplicación curricular de estas tecnologías, para lo que se continuará reforzando la capacitación de los docentes, completando la dotación de equipamiento y recursos digitales a cada plantel. Asimismo, en términos de cobertura, Enlaces tiene como norte incorporar a la red, al mundo rural, completando las escuelas básicas pertenecientes en su mayoría a zonas aisladas del país, con las estrategias y contenidos pertinentes a su realidad. |
| RJ11 | Conector de 4 contactos utilizado para conectar aparatos telefónicos. |
| RJ45 | Conector de 8 contactos utilizado para interconectar redes de |

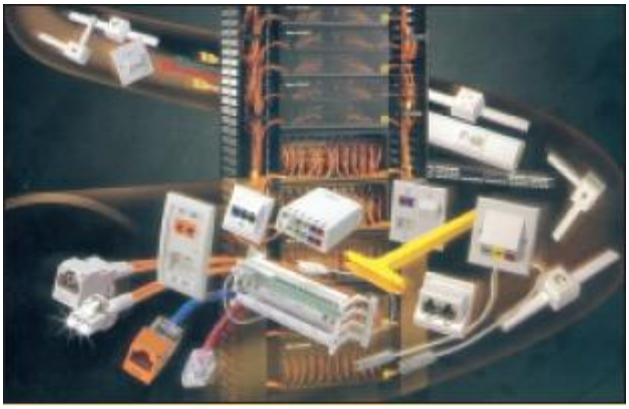
| | |
|---|---|
| | computadores basados en cable UTP. |
| ROUTER | Un router es una pieza de hardware o software que conecta dos o más redes. Asegura el encaminamiento de una comunicación a través de una red. |
| SIMPLEX | Transmisión de información en un solo sentido a través de un medio. |
| SLIP | Siglas de Serial Line Internet Protocol. SLIP es un protocolo que permite utilizar el TCP/IP en una línea telefónica por medio de un módem. |
| SPLITTER | Filtro utilizado en servicios de ADSL que permite diferenciar las frecuencias de voz y las frecuencias de datos. |
| SUBTEL | Subsecretaria de Telecomunicaciones. |
| T1 | Servicio de transporte digital usado para transmitir una señal a 1.544 Mbps. Una trama T1 tiene 24 ranuras de tiempo (timeslots) o canales. |
| TCP/IP | TCP/IP son las siglas de Transmission Control Protocol/Internet Protocol, el lenguaje que rige todas las comunicaciones entre todos los ordenadores en Internet. TCP/IP es un conjunto de instrucciones que dictan cómo se han de enviar paquetes de información por distintas redes. También tiene una función de verificación de errores para asegurarse que los paquetes llegan a su destino final en el orden apropiado. IP, Internet Protocol, es la especificación que determina hacia dónde son encaminados los paquetes, en función de su dirección de destino. TCP, o Transmission Control Protocol, se asegura de que los paquetes lleguen correctamente a su destino. Si TCP determina que un paquete no ha sido recibido, intentará volver a enviarlo hasta que sea recibido correctamente. |

| | |
|---|---|
| TIC | Tecnologías de información y comunicación. |
| TOPOLOGÍA | Arreglo lógico o físico de nodos o estaciones en una red. Existen diferentes topologías de red (bus, anillo, estrella, malla). |
| UNIDAD TRANSCEIVER | Transductor. Dispositivo que recibe la potencia de un sistema mecánico, óptico, electromagnético o acústico y lo transmite a otro, generalmente en forma distinta. El micrófono y el altavoz son ejemplos de transductores. En comunicaciones es un transmisor receptor de señales de radio frecuencia, ópticas o electromagnéticas. |
| UPSTREAM | Flujo de datos que es enviado desde un computador remoto a un servidor. |
| URL | Siglas de Uniform Resource Locator. Es la dirección de un sitio o de una fuente, normalmente un directorio o un fichero, en el World Wide Web y la convención que utilizan los navegadores para encontrar ficheros y otros servicios distantes. |
| USB | Universal Serial Bus. Tecnología plug-and-play que interconecta un computador con otros dispositivos (teclado, ratón, impresora) sin la necesidad de apagar el computador. La tecnología USB fue desarrollada por Compaq, IBM, DEC, Intel, Microsoft, NEC, y Northern Telecom. Un puerto USB soporta velocidades de conexión de 12 Mbps. |
| VIDEO CONFERENCIA | Sistema que permite la transmisión en tiempo real de video sonido y texto a través de una red, ya sea de área local (L.A.N.) o Internet. El hardware necesario es una tarjeta de sonido y video, video cámara, micrófono y parlantes. |
| VOIP | Voz sobre IP. Se refiere a tecnologías usadas por las empresas de telecomunicaciones para prestar servicios de telefonía utilizando la red |

| | |
|---|---|
| | Internet. |
| W.A.N. | Siglas de Wide Area Network. Red que conecta computadores distantes por medio de líneas telefónicas o por otro tipo de enlace. |
| WLL | Wireless Local Loop. Tecnología de acceso a Internet y telefonía mediante enlaces de radiofrecuencia por sobre los 3.400 Mhz. Permite velocidades desde los 128 Kbps. |
| WORLD WIDE WEB | Literalmente tela de araña mundial. Antes de aparecer este servicio, los usuarios de la red tenían que manejar toda una serie de comandos y poseer cierto nivel de conocimientos sobre sistemas operativos para poder hacer operaciones como copiar un archivo, mandar un mensaje. Al ir aumentando el número de usuarios se hizo necesario buscar herramientas que hicieran más sencillo el acceso a la información y el manejo de la misma. Se crearon servicios como GOPHER y World Wide Web. La ventaja de estos servicios fue su entorno gráfico y el poco uso de comandos escritos para realizar cualquier acción. Se puede considerar el web como una serie de archivos de texto, multimedia y otros servicios conectados entre sí por medio de un sistema de documentos de hipertexto. |
| X10 | Lenguaje de comunicación que utilizan los productos compatibles X10 para hablar entre ellos. Lo que permite controlar luces, electrodomésticos de un hogar, aprovechando para ello la instalación eléctrica existente del hogar u oficina. |
| XDSL | xDSL se refiere a un grupo similar de tecnologías que proveen ancho de banda sobre circuitos locales de cable de cobre, sin amplificadores o repetidores de señal a lo largo de la ruta del cableado, entre la conexión del cliente y el primer nodo en la red. |

# ANEXOS

# CABLEADO ESTRUCTURADO



## Equipos de Cableado Estructurado

**Patch Panels**
La solución usará Patch Panels cat 6 del tipo 110 de 24 puertos. Deberá cumplir y exceder los requerimientos de la norma TIA/EIA 568 B.2-1 para categoría 6 y tener una aprobación UL.

**Jacks Modulares montable en match Panels (550 unidades)**
Los jacks deben cumplir los estándares T568A - T568B y tener la aprobación UL, así mismo debe tener la calificación 94 V-0, estos deberán tener una notación escrita de ambos códigos de color y contar con dust covers. Deben permitir reutilizarlos por lo menos 200 reconectorizaciones y deberán soportar por lo menos 750 reinserciones del plug del patch cord al jack.
Los contactos deberán ser de aleación en cobre y berilio con un baño de oro de 50 micrones mínimo.

**Patch Cords**
Los patch cords deberán ser categoría 6 y 1.5 mts de longitud. Estos deberán ser de 24 AWG de cable multifilar, Deberá tener capuchas protectoras al plug RJ45 en ambos extremos de material Poliofileno Elastomérico. Deberán cumplir y exceder los requerimientos de la norma TIA/EIA 568 B.2-1 para categoría 6. Se recomienda que los plugs deben ser de bronce fosforado con un baño de 50 micrones de oro.

**Tomadatos ( Faceplates )**

Las placas tomadatos o faceplates deberán ser de material termoplástico con 45° de inclinación, debe incluir 2 puertos (uno para datos y otro para voz), el color debe cumplir las normas de cableado para data y voz. El cual debe incluir dos biseles para colocar etiquetas que permitan identificar al usuario en forma instantánea. Debe contar con una aprobación UL. , debe contener los jack modulares montados

**Organizadores Horizontales**

Los organizadores deben tener 2 RU, debe corresponder a los estándares de Cableado.


**Gabinetes de Piso (01 unidades)**

Gabinetes de altura completa que permitirán albergar a los equipos de cableado estructurado y comunicaciones, con las siguientes características:

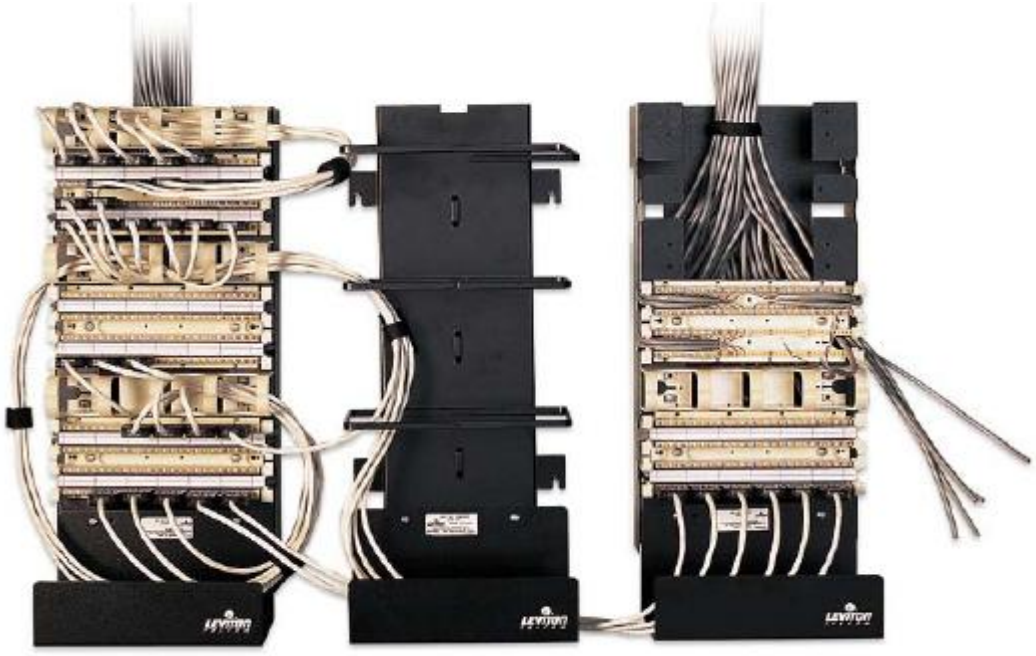
• Altura: 18-RU
• Construidos en plancha de acero laminado al frio – espesor 16.
• Puerta frontal con vidrio de seguridad de 5mm y marco de malla metálica con chapa y llave.
• Paneles lateral y posterior desmontables con ganchos de seguridad, y llave.
• Acabado en pintura electrostática, con acceso para cables en la parte superior e inferior.
• Debe posee un extractor de calor como mínimo
• Debe Cumplir las especificaciones de la norma EIA 310D.
• Color
• Certificación ISO 9001

**CERTIFICADOR DE CABLE DE COBRE Y FIBRA OPTICA**

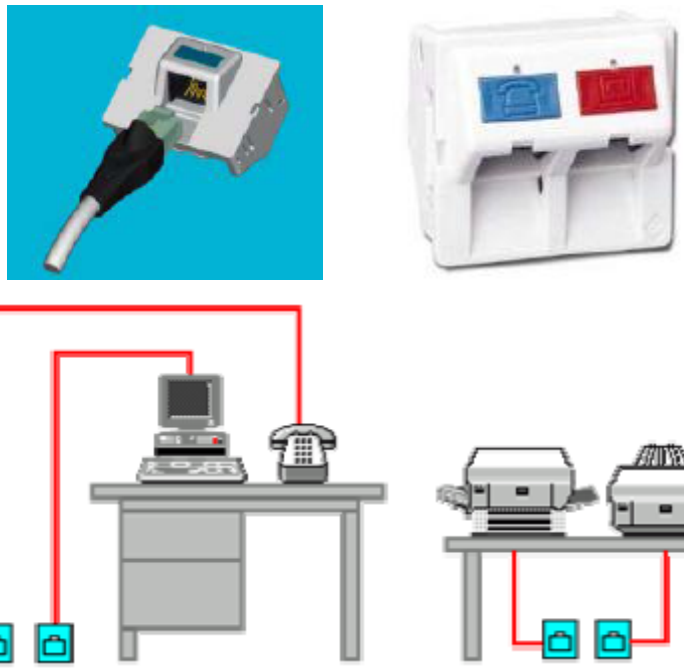
## Conexiones a un Patch Panel


## Colocación de los Equipos en un Rack

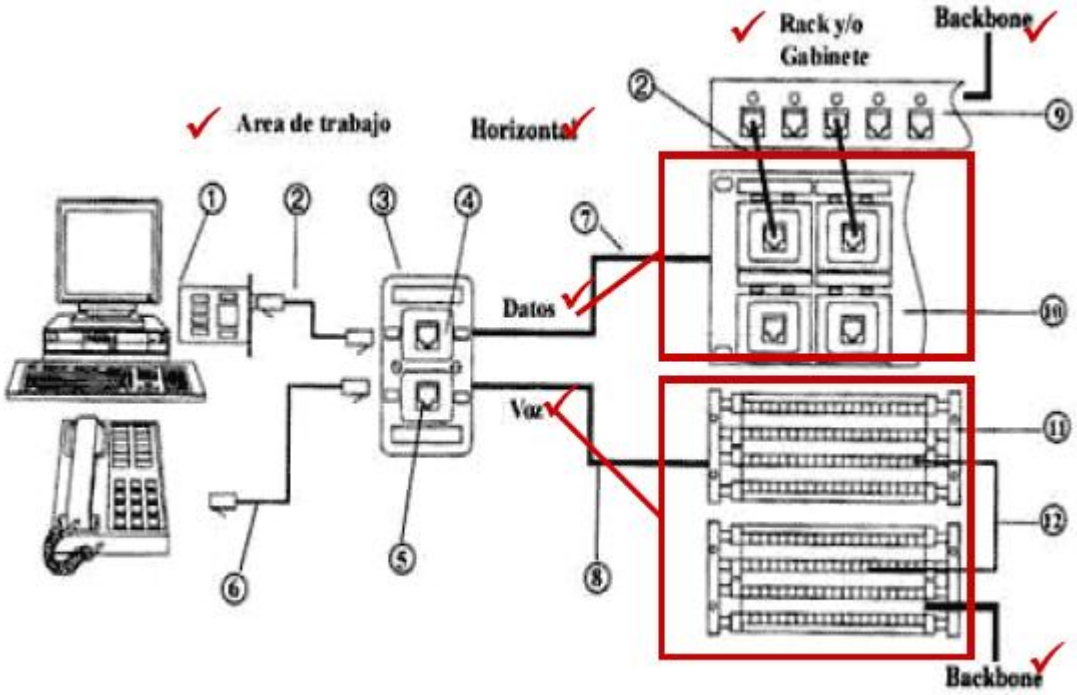
## Separadores y Soportes o Racks



## Conexiones DATA – VOZ (UTP Categoría 6)

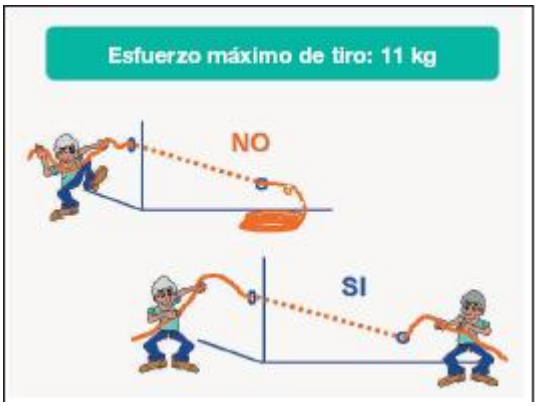


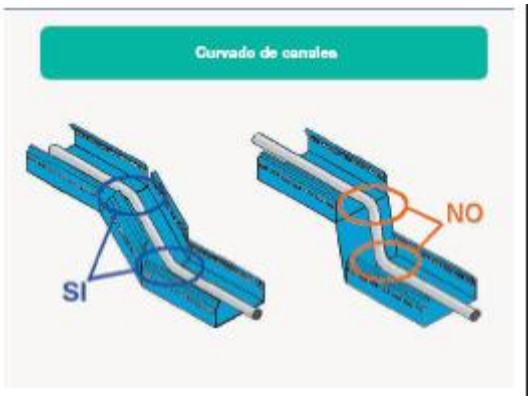
**Esquema de Conexiones Data - Voz**




**Forma de la Distribución del Cableado**

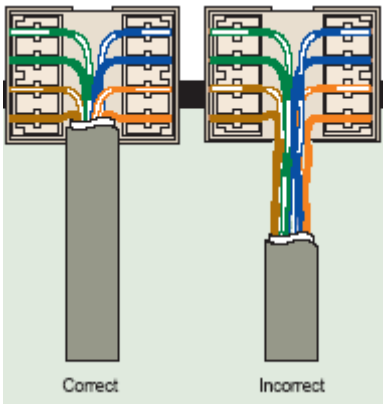
**Instalación de los Puntos de Red**

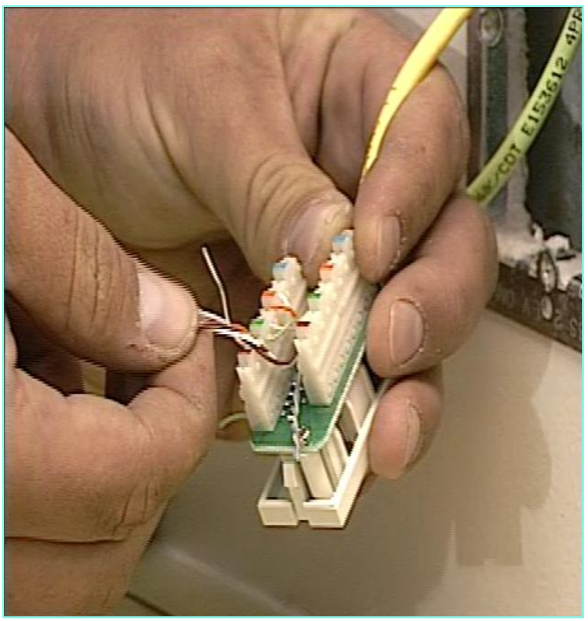


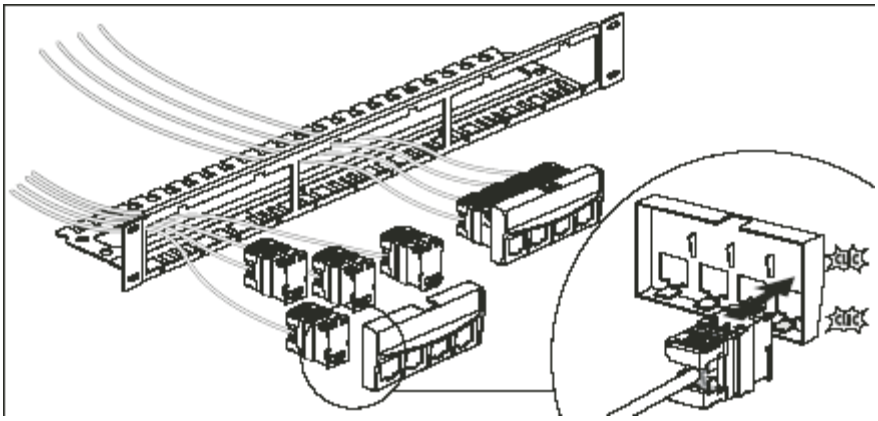

***Pase de los Cables por Ductos Internos y Canaletas***

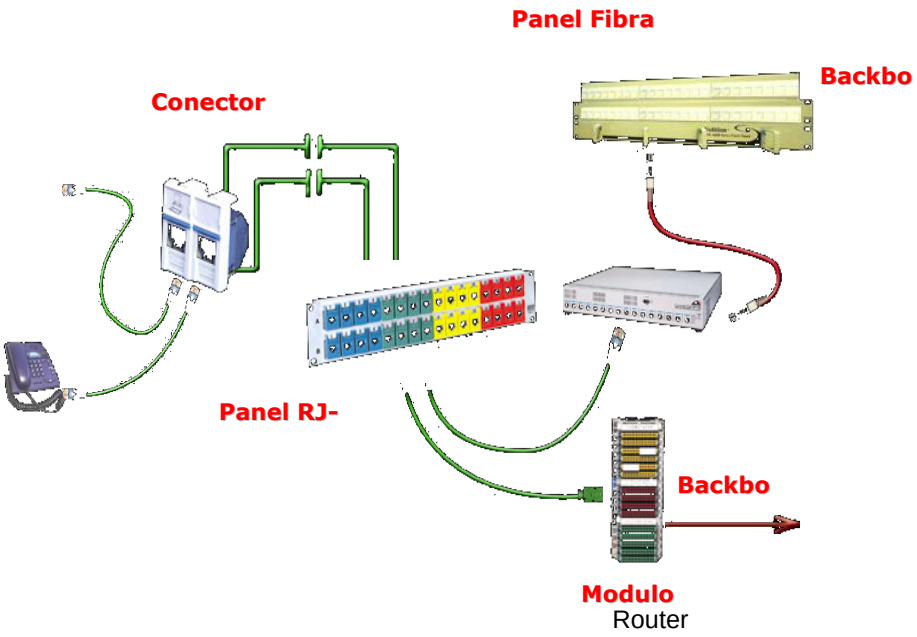
***Conexiones de los Puntos RJ45***
***- Usando la Ponchadora***



***- Usando Jack a presión para el Patch Panel en una Red Lan Básica***

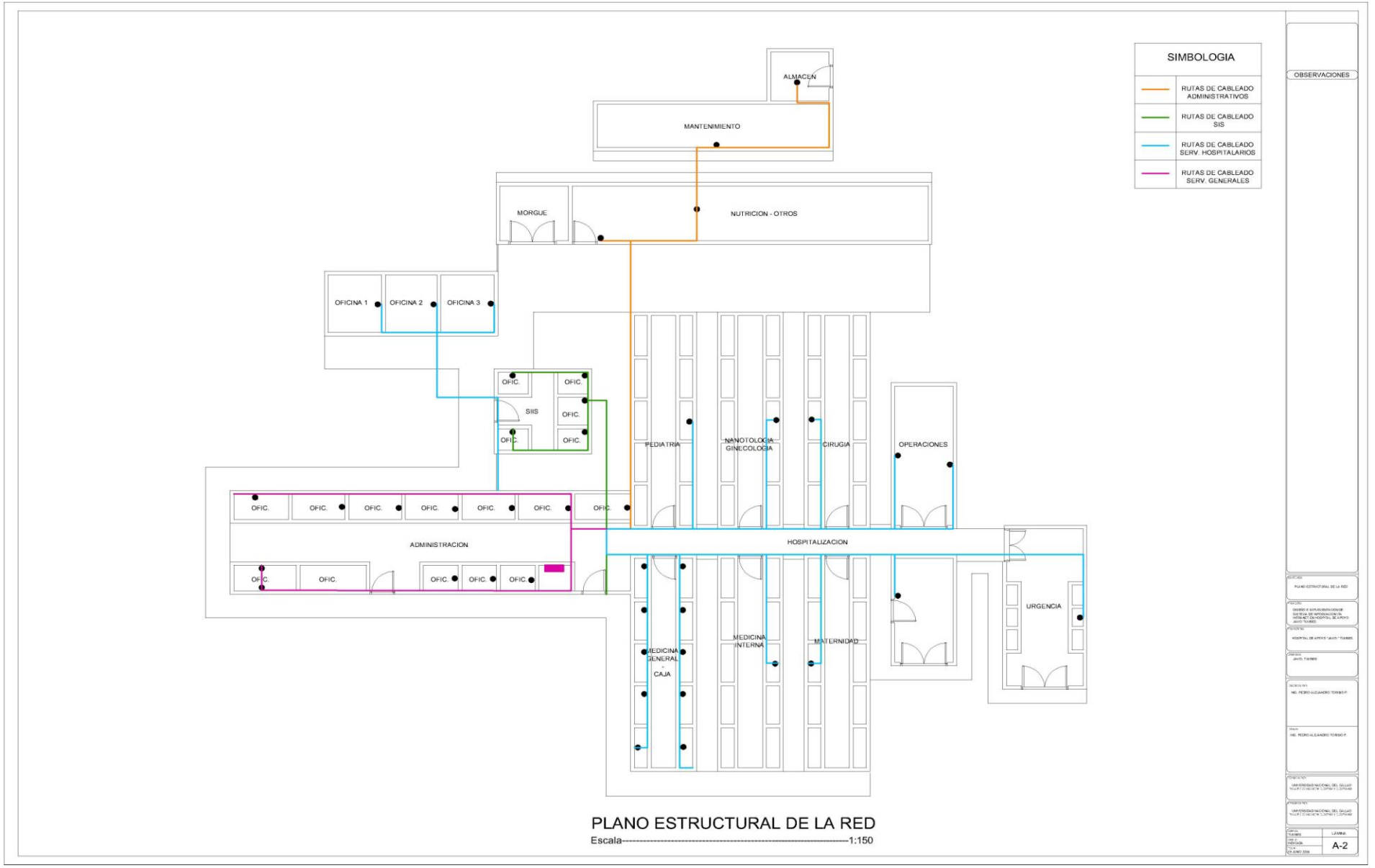
# PLANOS


DIAGRAMA DE RED ESTRELLA

Escala----------1:150

OBSERVACIONES

A-1


SIMBOLOGIA
RUTAS DE CABLEADO ADMINISTRATIVOS
RUTAS DE CABLEADO SIS
RUTAS DE CABLEADO SERV. HOSPITALARIOS
RUTAS DE CABLEADO SERV. GENERALES
OBSERVACIONES
ALMACEN
MANTENIMIENTO
MORGUE
NUTRICION - OTROS
OFICINA 1
OFICINA 2
OFICINA 3
OFIC.
SIIS
PEDIATRIA
NANOTOLOGIA GINECOLOGIA
CIRUGIA
OPERACIONES
ADMINISTRACION
HOSPITALIZACION
URGENCIA
MEDICINA GENERAL - CAJA
MEDICINA INTERNA
MATERNIDAD
PLANO ESTRUCTURAL DE LA RED
Escala----------1:150
A-2