
VNIVERSIDAD NACIONAL AVTNOMA DE MEXICO

# UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES

ARAGON

# EL PROTOCOLO ETHERNET A NIVEL INDUSTRIAL

## T E S I S

QUE PARA OBTENER EL TITULO DE:

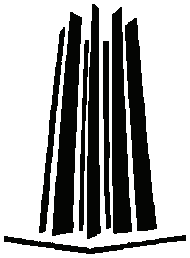
**INGENIERO MECANICO ELECTRICISTA**

**AREA: ELECTRICA-ELECTRONICA**

P R E S E N T A :

**HERNANDEZ CARDENAS EVERARDO VICTORINO**

ASESOR: ING. ENRIQUE GARCIA GUZMAN



MEXICO, 2007

# DEDICATORIA

**A Dios:**

*Por haberme regalado esta vida y forma de ser, las cuales no cambiaria por nada del mundo…*

**A mi papa Héctor Everardo Hernández Ocaña †:**

*Por ser el mejor ejemplo como persona, padre, amigo y ser humano que cualquier hijo puede desear…*

**A mi mama María de la Luz Cárdenas Reyes:**

*Por ser la persona que me trajo al mundo, me cuido y más me ha alentado a conseguir mis objetivos a pesar de las circunstancias y de las personas…*

**A mis hermanos Luz Andrea †, Héctor y Verenice:**

*Por su apoyo y ayuda cuando a veces uno lo necesita…*

**A Leticia Jaimes Acevedo:**

*Por darme la alegría que pensé había perdido…*

**A mis familiares:**

*Por los consejos, criticas y sobre todo cariño…*

**A mis amigos:**

*Por lograr acercarme a la realidad y buscar alternativas a los problemas…*

**A mi asesor; Ing. Enrique García Guzmán:**

*Por haberme esperado tanto tiempo para la conclusión de mi tesis, pero sobre todo por ser más mi amigo que profesor…*

**A la UNAM:**

*Porque todos merecemos una segunda oportunidad y tu me la diste…*

**A todos los profesores de la FES Aragón:**

*Por compartir tantos conocimientos conmigo…*

Índice

Pagina

**Capitulo 3 Protocolos industriales Ethernet selectos y aplicaciones**

## Introducción

Desde el inicio de la revolución industrial en el Siglo XIX la necesidad del hombre por controlar el medio que lo rodeaba lo llevo a utilizar maquinarias cada vez mas complejas, aunque con la creación de dichas maquinas se incrementaba de igual forma el riesgo que conllevaba el poder controlarlas y el riesgo para el personal que las manejaba. Fue durante mediados del Siglo XX cuando un invento revoluciono la forma tanto de trabajar como de controlar todo lo que hasta ese momento solo podía manejar personal calificado: la computadora.

En sus inicios el uso de la computadora se limito solo a investigaciones de tipo militar con la red pionera en switcheo de paquetes llamada ARPANET (Advanced Research Projects Agency Network) por lo que durante algunos años no fue posible desarrollar aplicaciones en otras ramas de la ciencia ni para su uso en casas, oficinas e incluso industrias.

Fue en la década de los ochentas cuando se dio un gran auge al uso de las computadoras sobre todo en universidades de Estados Unidos pues el uso de estas se extendió no solo al uso militar y así poco a poco cada vez mas gente conoció y se adentro en el uso de una tecnología virgen hasta ese momento.

Las primeras aplicaciones en las que se utilizo la computadora fue en cálculos y operaciones que día con día se volvieron mas complejas hasta el punto de tener que interconectar una o varias de estas computadoras para poder intercambiar archivos de datos los cuales recortaban los tiempos perdidos en llevar en papel los mismos de una oficina a otra dentro de un edificio o incluso a un edificio adjunto.

Fue así como se crearon las redes de oficina utilizando para esto un lenguaje común mediante el cual todas las computadoras dentro de la red pudieran entenderse y así poder intercambiar tareas como el compartir archivos e impresoras.
El nombre de este lenguaje mediante el cual se comunicaban las computadoras fue Ethernet (aunque no fue el único protocolo desarrollado en ese tiempo pero si el que prevalece hasta el día de hoy) y fue descrito como protocolo ya que se siguen una serie de reglas para poder establecer una comunicación exitosa entre dos o más computadoras conectadas a la red.

Durante casi una década y media (mediados de los 80's) el uso de la red Ethernet se limito al ámbito de la oficina pero con los avances cada vez mas rápidos en materia de incrementos de ancho de banda en la red, de velocidades de procesamiento de las CPU's y mejores materiales para la conexión y construcción de las redes de computadoras; este uso se extendió a la industria, ya que en esta las operaciones criticas tenían que ser controladas de una manera segura y efectiva, pues algunas tareas eran muy peligrosas para el personal operativo de las plantas industriales, y algunas empresas no podían darse el lujo de perder dinero ni vidas debido a tiempos muertos en su producción. Las empresas que en un inicio se interesaron sobremanera en el uso de las redes de computadoras fueron las del petróleo, químicas, armadoras de automóviles, del cemento, etc.

Atendiendo a la necesidad cada vez mayor de estar informados acerca de los nuevos retos y avances técnicos de las comunicaciones que se desarrollan a nivel mundial en el ramo de la industria, el presente trabajo pretende ser una guía para establecer los criterios mas importantes a la hora de escoger el tipo de protocolo Ethernet conveniente a las necesidades industriales dependiendo de algunos criterios generales que son comunes a todas ellas al momento de escoger el protocolo de comunicación optimo a sus necesidades.

En el primer capitulo se muestran la historia, características y principios básicos bajo los cuales el protocolo Ethernet a nivel oficina opera y hace posible la comunicación entre computadoras tanto en una misma red interna (LAN) como de otros tipos como son las MAN (Metropolitan Area Network), WAN (Wide Area Network), etc., así como su evolución hasta 10Gigabit Ethernet.

En el segundo capitulo se aborda de lleno el protocolo Ethernet aplicado a la industria señalando características diferentes entre el uso en la oficina y el uso en la industria, así como términos los cuales son muy importantes en las aplicaciones industriales como es el tiempo real, las estructuras de comunicación, tipo de cableado industrial, etc.

Por ultimo en el capitulo tres se señalan las diversas variaciones del protocolo Ethernet basadas en el mismo debidas al desarrollo separado por parte de distintas empresas a nivel mundial dándole cada una de ellas prioridad a distintos detalles relativos al protocolo para hacer así mas efectivo el uso del mismo en diferentes campos a nivel industrial. También se abordan tres casos de aplicación en los que diferentes empresas reconocidas a nivel mundial implementaron con éxito el protocolo Ethernet.

## Objetivo general

Conocer el principio de funcionamiento del protocolo Ethernet tanto en el nivel oficina como a nivel industrial para así formar los criterios de evaluación necesarios que se toman en cuenta al elegir el protocolo industrial Ethernet correcto.

### Objetivos particulares

- Relatar la historia del protocolo Ethernet desde sus inicios.
- Exponer la teoría de operación sobre la cual trabaja dicho protocolo a nivel oficina e industria.
- Emplear este conocimiento para analizar y así diferenciar mediante casos de aplicación prácticos las cualidades que distinguen a Ethernet industrial.
- Definir las bases mínimas necesarias para escoger el protocolo industrial correcto.

### Justificación del tema

Dar a conocer la importancia del protocolo en el desarrollo industrial basado en los datos de los diferentes fabricantes y desarrolladores de la tecnología Ethernet que están adscritos a la IAONA – Industrial Automation Open Networking Alliance, organización europea dedicada a promover y extender el uso de Ethernet a nivel industrial en todo el mundo.

Extender esta información a la mayoría de ingenierías que confluyen con este tema como son: Ingeniería Mecánica - Eléctrica, Ingeniería en Computación, Ingeniería en Control y Automatización, etc. Para de este modo estar de la mejor forma posible informados acerca de los cambios que se dan con respecto a la tecnología de redes a nivel industrial y así poder formar los criterios necesarios para elegir el protocolo Ethernet industrial que puede ayudarnos al momento de querer actualizar una industria no importando el rol al que se dedique la misma.

Difundir las características principales del protocolo con la finalidad de que sean estas una guía sencilla tanto de uso como de acceso al no haber información en el idioma español que pueda ser conseguida fácilmente, ya que México es un país consumidor de tecnología mediante la cual generalmente las compañías extranjeras solo venden su solución tecnológica pero la información de por que una solución es mejor que otra no se difunde fácilmente, llegando a veces a caer en la cuenta de que la solución no era la correcta por “falta de información acerca de la solución”.

# CAPITULO 1

## Principios básicos de operación del protocolo Ethernet

## 1.1 Ethernet —Una Breve Historia

Más de 30 años atrás -a principios de los 70's- Bob Metcalfe de Xerox Palo Alto Research Center (PARC) desarrolló un mecanismo de interconexión para una impresora Xerox y algunas computadoras vía un medio de comunicación. Para la nueva red él usó técnicas de escucha simultánea y habla mutua en un canal común de radiocomunicación.

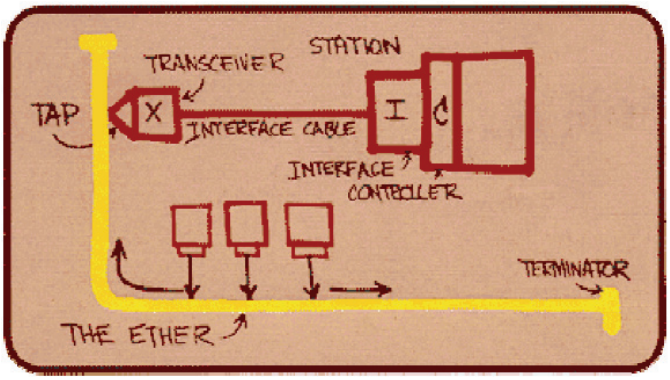



***Figura 1-1 Idea original de Bob Metcalfe de Ethernet***

Este principio llamado CSMA/CD (Carrier Sense Multiple Access/Colission Detection), es el principio básico de Ethernet hasta hoy en día. El nombre Ethernet resultó de la derivación de la tecnología de radio: en el siglo XIX muchos científicos creían que las ondas electromagnéticas necesitaban un medio de propagación y ese medio fue llamado "Ether".
Los primeros sistemas Ethernet fueron capaces de conectar más de 100 estaciones con un cable de más de 1000 m y realizaban una transferencia de datos de 3 MBits/segundo. Basado en esa investigación, el grupo DIX que era un consorcio de las compañías DEC, Intel y Xerox empezaron al final de los setentas con el mejoramiento de Ethernet para una tasa de datos de 10 MBits/seg. Dentro del desarrollo mientras tanto las tasas de datos de 1000 Megabit/seg para Gigabit Ethernet y 10,000 MB/seg para la 10 Gigabit Ethernet fueron conseguidas. En estas redes no sólo cables coaxiales, también cable de par trenzado, cables de fibra óptica y transmisión sin cable es utilizada. Aun las redes Ethernet mas rápidas con tasas de transmisión arriba de 100 Gigabit/segundo o más están ya planeadas.

El IEEE (Instituto de Ingenieros Eléctricos y Electrónicos por sus siglas en ingles) basado en Nueva York ha tomado la responsabilidad de la estandarización y coordinación de la familia de tecnologías de Ethernet lo cual hizo posible liberar, basado en los resultados de trabajo del grupo DIX el primer estándar Ethernet IEEE 802.3 en 1983. Desde entonces, el estándar Ethernet fue consistentemente extendido por el IEEE. Los estándares correspondientes están sujetos a un continuo desarrollo y mejoramiento por suplementos.
Dentro de la *Tabla 1-1* figuran los estándares más importantes de Ethernet:

| | |
|---|---|
| 1972 | Comienzo del desarrollo por Xerox |
| 1976 | Primera presentación (Tasa de datos a 3 MB/s) |
| 1980 | Standard "Ethernet V1.0" (DIX) |
| 1983 | Standard IEEE 802.3 |
| 1990 | Ethernet en Par Trenzado (10Base T) |
| 1995 | Fast Ethernet (100Base-X) |
| 1998 | Gigabit-Ethernet (1000BaseT) |
| 2002 | 10 Gigabit-Ethernet |

***Tabla 1-1 Evolución de los estándares Ethernet***

En la actualidad, Ethernet es usado en la mayoría de redes locales en el área de oficina (Local Area Network, LAN) y es también la columna vertebral para Internet.
En comparación a esta original área de aplicación, en los últimos años Ethernet se expande más y más en el área de automatización industrial, donde primariamente el problema de velocidad y comunicación deterministica ha sido resuelto.

## 1.2 Estándares bajo los que opera la red Ethernet

A continuación se muestran todos los estándares que utiliza Ethernet para su funcionamiento:

| Standard | Comentarios |
|---|---|
| IEEE 802.1 | Modo de trabajo de Internet (Puenteo & Gestión), Bridging & Management |
| IEEE 802.2 | Control de Link o Enlace Lógico, Logical Link Control (LLC) |
| IEEE 802.3 | Primer Standard Ethernet (Método de Acceso CSMA/CD) |
| IEEE 802.3a | Medio de transmisión 10Base2, cable coaxial delgado (BNC) |
| IEEE 802.3b | Medio de transmisión 10Broad36, banda ancha vía canales de TV por cable |
| IEEE 802.3c | Repetidor a 10 Mbit/s para 10Base2 y 10Base5 |
| IEEE 802.3d | Enlace de fibra Punto-a-Punto entre 2 repetidores |
| IEEE 802.3e | 1Base5, Topología en estrella, cableado de par trenzado |
| IEEE 802.3h | Gestión de Capas |
| IEEE 802.3i | 10Base10, cableado de par trenzado, 10 Mbit/s |
| IEEE 802.3j | Enlace de fibra 10BaseF con hubs activos/pasivos, posible operación full-duplex parcial |
| IEEE 802.3k | Administración del repetidor |
| IEEE 802.3q | Directrices para el Desarrollo de Administración de Objetos |
| IEEE 802.3u | Fast Ethernet, 100BaseT, FX (2 x fibra multimodo), TX (2 pares de cables), T4 (4 pares de cables |
| IEEE 802.3x | Full-duplex (10/100/1000 Mbit/s y autonegociación) |
| IEEE 802.3z | Gigabit Ethernet, 1000BaseT, SX (2 Fibras multimodo o monomodo), LX (2 x Fibra Monomodo), CX (2 pares de cables) |
| IEEE 802.3ae | 10 Gigabit Ethernet |
| IEEE 802.3af | Energía sobre Ethernet (Power over Ethernet) |
| IEEE 802.11 | Wireless LAN (WLAN) |
| IEEE 802.15.1 | Bluetooth |
| IEEE 802.15.4 | ZigBee |

***Tabla 1-2 Estándares Ethernet***

## 1.3 Elementos de la Red Ethernet

Las redes de área local Ethernet consisten en nodos de red y los medios de interconexión. Los nodos de red caen en dos clases importantes:

- **Dispositivos de equipo terminal de datos (DTE)** – Aparatos que son la fuente o el destino de los datos. Los DTEs son típicamente dispositivos tales como PC, estaciones de trabajo, servidores de archivos, o servidores de impresión que, como un grupo, sean todos referidos a menudo como estaciones finales.

- **Dispositivos de comunicación de datos (DCE)** – Aparatos intermedios que reciben y remiten datos a través de la red. Los DCEs pueden ser dispositivos independientes tales como repetidores, interruptores de red (switches), y ruteadores, o unidades de interfaz de comunicaciones tales como tarjetas de interfaz y módems.

A través de este capítulo, los dispositivos intermedios independientes de la red serán referidos como *nodos intermedios* o *DCEs*. Las tarjetas de interfaz de la red serán referidas como *NICs*.
Las opciones actuales de los medios de Ethernet incluyen dos tipos generales de cable de cobre: par trenzado no blindado (UTP Unshielded Twisted-Pair) y par trenzado blindado (STP Shielded Twisted-Pair), más varios tipos de cable de fibra óptica.

## 1.4 Topologías y estructuras de la red Ethernet

Las LANs toman muchas configuraciones de topologías, pero sin importar su tamaño o complejidad, todo será una combinación de solamente tres estructuras de interconexión básicas o bloques de construcción de red.

La estructura más simple de interconexión es la punto a punto, mostrada en la *Figura 1-2*. Solamente dos unidades de red están implicadas, y la conexión puede ser DTE-DTE, DTE-DCE, o DCE-DCE. El cable en las conexiones punto a punto se le conoce como acoplamiento de la red. La longitud máxima permitida del acoplamiento depende del tipo de cable y del método de transmisión que es utilizado.


***Figura 1-2 Ejemplo de conexión Punto a Punto***

Las redes Ethernet originales fueron implementadas con una estructura de bus coaxial, como se muestra en la *Figura 1-3*. Las longitudes de segmento fueron limitadas a 500 metros, y hasta 100 estaciones se podrían conectar con un solo segmento. Segmentos individuales se podrían interconectar con repetidores, tan largo como las trayectorias múltiples que existían entre dos estaciones en la red y el número de DTEs no excedían de 1024. La distancia total de la trayectoria entre el par de estaciones mas distante también no fue permitida a exceder un valor máximo prescrito.

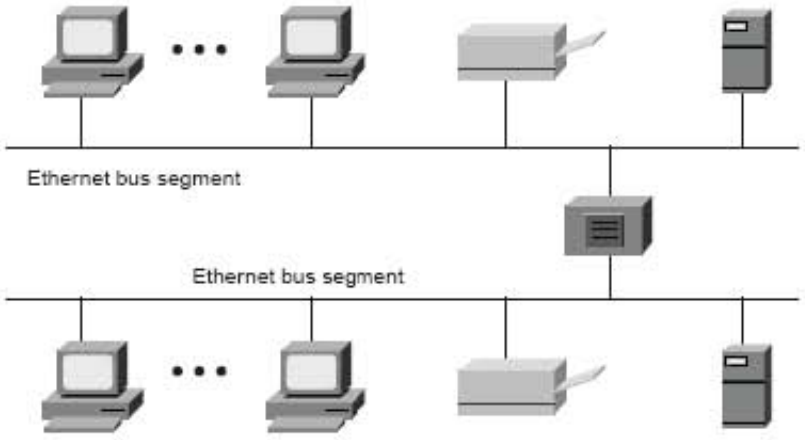



***Figura 1-3 Ejemplo de Topología de Bus Coaxial***

Aunque las nuevas redes no son más largas conectadas en una configuración de bus, algunas redes más viejas conectadas en bus siguen existiendo y aun son útiles.

Desde principios de los años 90, una opción de la configuración de red ha sido la topología en estrella, mostrada en la *Figura 1-4*. La unidad central de la red es o un repetidor de multipuerto (también conocido como hub) o un switch de red. Todas las conexiones en una red en estrella son enlaces punto a punto implementados con par trenzado o con cable de fibra óptica.

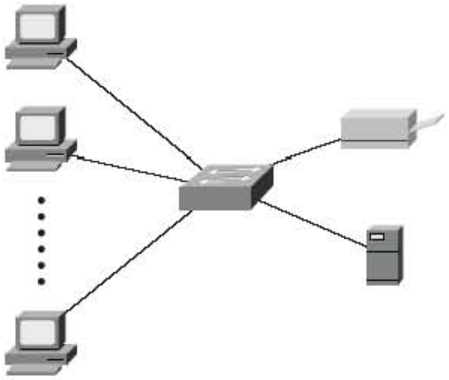


*Figura 1-4 Ejemplo de topología en Estrella*

En el capitulo siguiente se darán mas a detalle las estructuras de comunicación tanto físicas como lógicas en las que se basa el funcionamiento de Ethernet a nivel industrial.

## 1.5 La relación lógica del estándar IEEE 802.3 al modelo de referencia ISO

La *Figura 1-5* muestra las capas lógicas IEEE 802.3 y su relación al modelo de referencia OSI. Como todos los protocolos IEEE 802, la capa de enlace de datos ISO se divide en dos subcapas IEEE 802, la subcapa de Control de Acceso al Medio (MAC Media Access Control) y la subcapa de cliente MAC. La capa física (PHY) de la IEEE 802.3 corresponde a la capa física de la OSI.

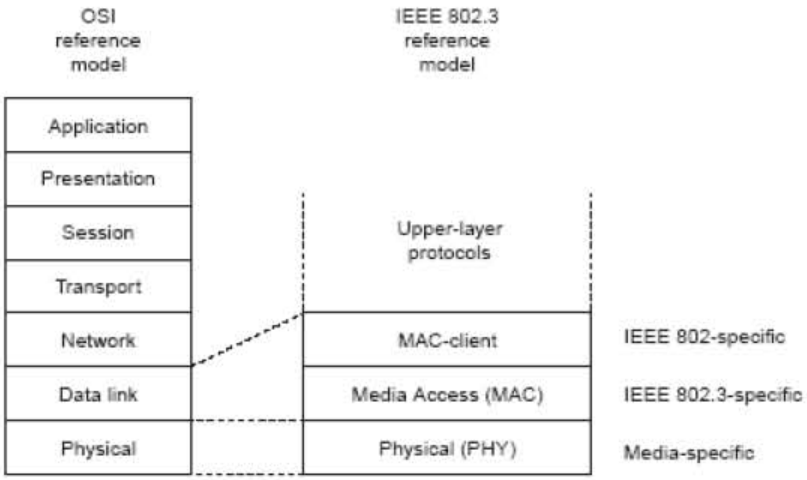



*Figura 1-5 Relación lógica entre Ethernet y el Modelo de Referencia ISO*

La subcapa de cliente MAC puede ser una de las siguientes:

- **Control de Enlace Lógico (LLC Logical Link Control)**, si la unidad es un DTE. Esta subcapa proporciona la interfaz entre el MAC de Ethernet y las capas superiores en la pila del protocolo de la estación del final. La subcapa del LLC es definida por los estándares IEEE 802.2.

- **Entidad de puente o bridge**, si la unidad es un DCE. Las entidades puente o bridge proporcionan las interfaces LAN-a-LAN entre LANs que usan el mismo protocolo (por ejemplo, Ethernet a Ethernet) y también entre diferentes protocolos (por ejemplo, Ethernet a Token Ring). Las entidades de puente están definidas por los estándares IEEE 802.1.

Debido a que las especificaciones para las entidades LLC y puente son comunes para todos los protocolos LAN IEEE 802, la compatibilidad de red se convierte en la responsabilidad primaria del protocolo particular de red. La *Figura 1-6* muestra diversos requisitos de compatibilidad impuestos por el MAC y los niveles físicos para la comunicación de datos básica sobre enlaces Ethernet.

La capa del MAC controla el acceso del nodo a los medios de la red y es específica al protocolo individual. Todas las MAC's IEEE 802.3 deben conocer los mismos requerimientos lógicos básicos, sin importar si ellos incluyen una o más de las extensiones opcionales definidas del protocolo. El único requisito para la comunicación básica (comunicación que no requiere extensiones opcionales de protocolo) entre dos nodos de red son que ambas MAC's deben soportar la misma tasa de transmisión.

La capa física 802.3 es específica a la tasa de transmisión de datos, a la codificación de la señal, y al tipo de medio de interconexión entre dos nodos. Gigabit Ethernet, por ejemplo, esta definido para funcionar sobre par trenzado o cable de fibra óptica, pero cada tipo especifico de cable o de procedimiento de codificación de señal requieren una distinta implementación de capa física.

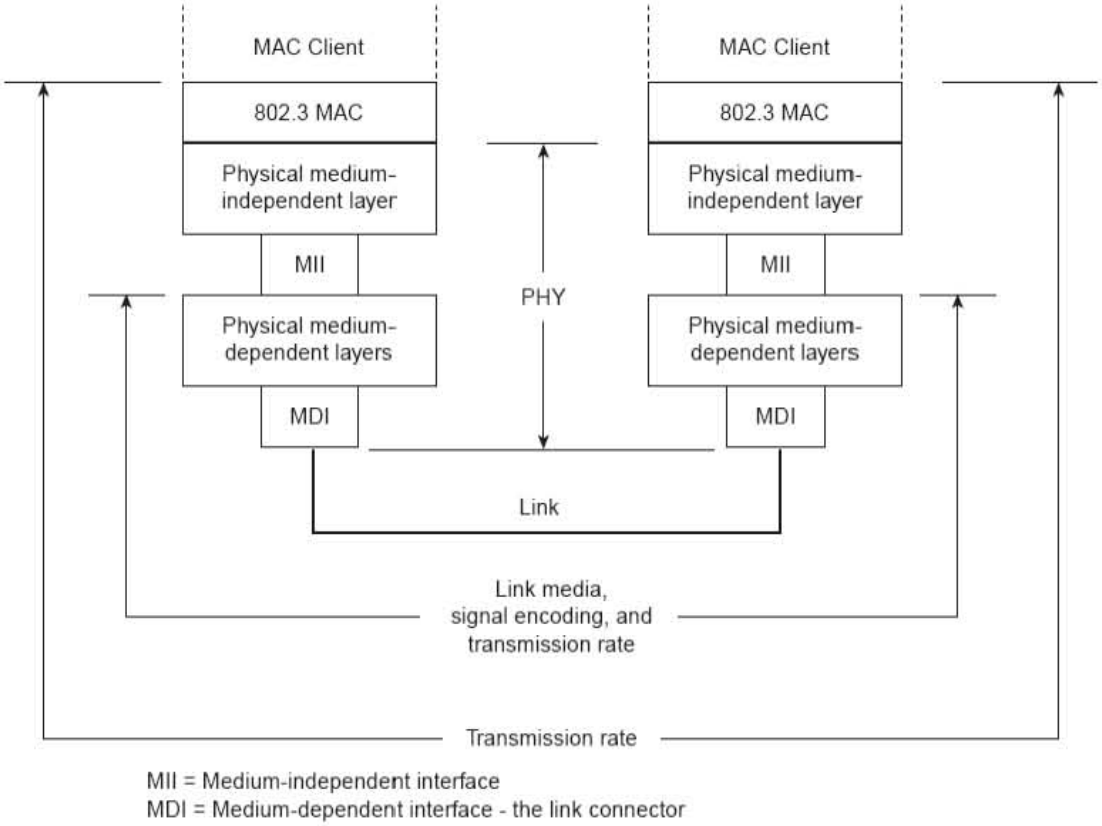



***Figura 1-6 Requerimientos de compatibilidad entre la Capa física y la Capa MAC para una comunicación básica***

## 1.6 La subcapa MAC de Ethernet

La subcapa MAC tiene dos responsabilidades primarias:

- Encapsulación de datos, incluyendo ensamblado de trama antes de la transmisión, y detección de error de sintaxis (parsing/error) de trama durante y después de la recepción
- Control de Acceso al Medio, incluyendo la iniciación de la transmisión de trama y de la recuperación desde la falla de transmisión

### 1.6.1 El formato básico de la trama de Ethernet

El estándar de IEEE 802.3 define un formato básico de la trama de datos que se requiere para todas las implementaciones de MAC, más varios formatos opcionales y adicionales que se usan para ampliar la capacidad básica del protocolo.

El formato básico de la trama de datos contiene los siete campos mostrados en la *Figura 1-7*.

- **El preámbulo (Preamble, PRE)** — Consiste en 7 bytes. El preámbulo es un patrón de unos y ceros alternados que dice a las estaciones receptoras que está viniendo una trama, y este proporciona medios para sincronizar las porciones de recepción de trama de las capas físicas con el flujo de bits entrantes.

- **Delimitador de inicio de trama (Start-Of-Frame, SOF)** — Consiste en 1 byte. El SOF es un patrón que alterna unos y ceros, terminando con dos bits 1 consecutivos que indican que el bit siguiente es el bit de más a la izquierda en el byte de más a la izquierda de la dirección de destino.

- **La dirección de destino (Destination Address, DA)** — Consiste en 6 bytes. El campo DA identifica qué estación(es) deben recibir la trama. El bit de mas a la izquierda en el campo de DA indica si la dirección es una dirección individual (indicada por un 0) o un grupo de direcciones (indicada por un 1). El segundo bit de la izquierda indica si la DA esta globalmente administrada (indicado por un 0) o localmente administrada (indicado por un 1). Los 46 bits restantes son un valor único asignado que identifica una sola estación, un grupo definido de estaciones, o todas las estaciones en la red.

- **La dirección de la fuente (Source Addresses, SA)** — Consiste en 6 bytes. El campo del SA identifica la estación que envía. La SA es siempre una dirección individual y el bit de más a la izquierda es siempre 0.

- **Largo / Tipo (Length / Type)** — Consiste en 2 bytes. Este campo indica si el número de bytes de datos del cliente MAC están contenidos en el campo de datos de la trama, o el tipo identificador de la trama si la trama está ensamblada usando un formato opcional. Si el valor del campo de Largo/Tipo es menor o igual a 1500, el número de los bytes del LLC en el campo de datos es igual al valor del campo de Largo/Tipo. Si el valor del campo de Largo/Tipo es mayor a 1536, la trama es de un tipo opcional, y el valor del campo identifica el tipo particular de trama siendo enviado o recibido.

- **Datos (Data)** — Es una secuencia de n bytes de cualquier valor, donde n es menor o igual a 1500. Si la longitud del campo de datos es menor a 46, el campo de datos debe ser extendido agregando un relleno suficiente para traer la longitud del campo de datos a 46 bytes.

- **Secuencia de chequeo de trama (Frame Check Sequence, FCS)** – Consiste en 4 bytes. Esta secuencia contiene un chequeo de redundancia cíclica de 32 bits (CRC), el cual es creado por la MAC que envía y recalculado por la MAC de recepción para comprobar si hay tramas dañadas. El FCS se genera sobre los campos DA, SA, y Largo/Tipo.

**Nota**
Las direcciones individuales también se conocen como direcciones unicast porque se refieren a una sola MAC y son asignadas por el fabricante del NIC desde un bloque de direcciones asignadas por el IEEE. Las direcciones del grupo (conocidas como direcciones multicast) identifican las estaciones terminales en un grupo de trabajo y son asignadas por el encargado de la red.
Una dirección especial de grupo (todos 1s — la dirección de difusión) indica todas las estaciones en la red.

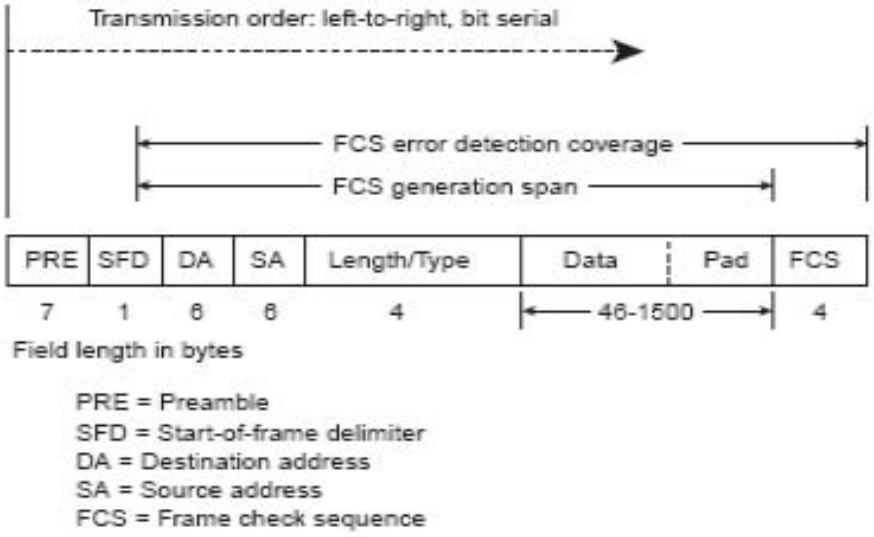



***Figura 1-7 Formato básico de la trama de datos MAC IEEE 802.3***

### 1.6.2 Transmisión de trama

Siempre que una estación MAC final recibe una petición de transmisión de trama con la dirección de acompañamiento y la información de datos desde la subcapa LLC, la MAC comienza la secuencia de transmisión enviando la información del LLC al buffer de trama MAC.

- El preámbulo y el delimitador de inicio de trama son insertados en los campos PRE y SOF.
- Las direcciones fuente y destino se insertan en los campos de dirección.
- Los bytes de datos del LLC son contados, y el número de bytes es insertado en el campo de Largo/Tipo.
- Los bytes de datos del LLC son insertados en el campo de datos. Si el número de bytes de datos del LLC es menor a 46, un relleno se suma para traer la longitud del campo de datos arriba de 46.
- Un valor de FCS es generado sobre la DA, SA, de Largo/Tipo, y campos de datos y es añadido al final del campo de datos.

Después de que la trama es ensamblada, la transmisión actual de trama dependerá de si la MAC está funcionando en modo half-duplex o full-duplex.

El estándar de IEEE 802.3 requiere actualmente que todos las MAC's Ethernet soporten la operación half-duplex, en la cual la MAC puede estar transmitiendo o recibiendo una trama, pero no puede hacer ambos simultáneamente. La operación full-duplex es una capacidad opcional de la MAC que permite que la MAC transmita y reciba tramas simultáneamente.

### 1.6.3 Transmisión Half-Duplex — El método de acceso CSMA/CD

El protocolo CSMA/CD fue desarrollado originalmente como un medio por el cual dos o más estaciones podrían compartir un medio común en un ambiente sin switches cuando el protocolo no requiere arbitraje central, toques de acceso o slots de tiempo asignados para indicar cuando una estación este lista para transmitir. Cada MAC Ethernet determina por sí misma cuando esta apta para enviar una trama.

Las reglas de acceso CSMA/CD son resumidas por las siglas del protocolo:

- **Sensor de portadora (CS, Carrier Sense)** — Cada estación escucha continuamente tráfico en el medio para determinar cuando ocurren vacíos de transmisión de tramas.

- **Acceso múltiple (MA, Múltiple Access)** — Estaciones pueden comenzar transmitiendo a cualquier momento detectando que la red esta silenciosa (no hay tráfico).

- **Detección de colisión (CD, Collision Detect)** — Si dos o más estaciones en la misma red CSMA/CD (dominio de colisión) comienzan a transmitir en aproximadamente el mismo tiempo, los flujos de bits de las estaciones transmisoras interferirá (chocara) con cada una, y ambas transmisiones serán ilegibles. Si sucede eso, cada estación transmisora debe ser capaz de detectar que ha ocurrido una colisión antes de que haya acabado de enviar su trama. Cada una debe parar la transmisión tan pronto como ha detectado la colisión y entonces debe esperar un tiempo aleatorio (determinado por un algoritmo de back-off) antes de procurar retransmitir la trama.

La peor situación ocurre cuando las dos estaciones más distantes en la red necesitan enviar una trama y cuando la segunda estación no comienza a transmitir hasta solo momentos antes de que la trama de la primera estación llegue. La colisión será detectada casi inmediatamente por la segunda estación, pero no será detectada por la primera estación hasta que la señal corrupta se ha propagado por todo el camino de regreso a esa estación. El tiempo máximo que se requiere para detectar una colisión (la ventana de colisión, o "time slot") es aproximadamente igual a dos veces al tiempo de la señal de propagación entre las dos estaciones más distantes en la red.

Esto significa que la longitud mínima de trama y el diámetro máximo de colisión están relacionados directamente con el time slot. Longitudes mínimas más largas de trama se traducen a slot times y diámetros más grandes de colisión; longitudes mínimas más cortas de trama corresponden a slot times más cortos y diámetros de colisión más pequeños.

El cambio estaba entre la necesidad de reducir la recuperación del impacto de la colisión y la necesidad de diámetros de red suficientemente grandes para acomodar tamaños razonables de red. El compromiso era elegir un diámetro máximo de red (cerca de 2500 metros) y después fijar la longitud mínima de la trama larga lo suficiente para asegurar la detección de todas las colisiones en el peor caso.

El compromiso trabajó bien para 10 Mbps, pero era un problema para desarrollos de tasas más altas de transferencia Ethernet. Fast Ethernet fue requerida para proveer compatibilidad hacia redes Ethernet anteriores, incluyendo el formato de trama existente IEEE 802.3 y procedimientos de error-detección, más todas las aplicaciones y software de red que funcionaban en las redes de 10 Mbps.

Aunque la velocidad de propagación de la señal es esencialmente constante para todas las tasas de transmisión, el tiempo requerido para transmitir una trama esta inversamente relacionada con la tasa de transmisión. A 100 Mbps, un largo mínimo de trama puede ser transmitido en aproximadamente una décima del tiempo definido del slot time, y ninguna colisión que ocurriera durante la transmisión no sería detectada probablemente por las estaciones que transmiten. Esto alternadamente, significó que los diámetros máximos de la red especificados para las redes de 10 Mbps podrían no ser utilizados para las redes a 100 Mbps. La solución para Fast Ethernet era reducir el diámetro máximo de la red por aproximadamente un factor de 10 (un poco más de 200 metros).

El mismo problema también surgió durante el desarrollo de la especificación para Gigabit Ethernet, pero disminuía los diámetros de red por otro factor de 10 (a aproximadamente 20 metros) para la operación a 1000 Mbps pero simplemente no era práctica.

Esta vez, los desarrolladores eligieron mantener aproximadamente los mismos diámetros máximos de dominio de colisión como en redes de 100 Mbps y aumentar el tamaño aparente mínimo de trama agregando un campo de extensión variable de no datos a tramas que son más cortas que la longitud mínima (el campo de extensión se quita durante la recepción de la trama).

La *Figura 1-8* muestra el formato de trama MAC con el campo de extensión Gigabit, y la *Tabla 1-3* muestra el efecto de la compensación entre la tasa de transmisión de datos y el tamaño mínimo de la trama para 10 Mbps, 100 Mbps y Ethernet a 1000 Mbps.

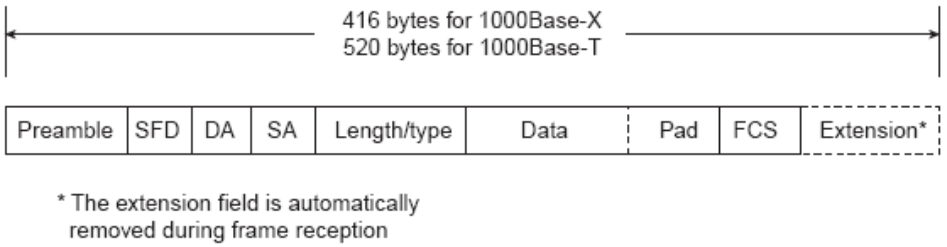



***Figura 1-8 Trama MAC con extensión de portadora Gigabit***

| **Parámetro** | **10 Mbps** | **100 Mbps** | **1000 Mbps** |
|---|---|---|---|
| Tamaño mínimo de trama | 64 Bytes | 64 Bytes | 520 Bytes[1] (sumada con extensión de campo) |
| Diámetro máximo de colisión, DTE a DTE | 100 metros UTP | 100 metros UTP<br>412 metros fibra | 100 metros UTP<br>316 metros fibra |
| Diámetro máximo de colisión con repetidores | 2500 metros | 205 metros | 200 metros |
| Numero máximo de repetidores en una trayectoria de red | 2500 metros | 205 metros | 200 metros |

[1] 520 bytes aplica a implementaciones 1000Base-T. el tamaño mínimo de trama con campo de extensión para 1000Base-X es reducido a 416 bytes porque 1000Base-X codifica y transmite 10 bits por cada byte

***Tabla 1-3 Limites para la operación Half-duplex***

Otro cambio a la especificación de transmisión Ethernet CSMA/CD era la adición de tramas en ráfaga (burst) para la operación de Gigabit. El modo de ráfaga es una característica que permite a una MAC enviar una secuencia corta (una ráfaga) de tramas igual a aproximadamente 5.4 tramas de longitud máxima sin tener que abandonar el control del medio.
La MAC transmisora llena cada intervalo intertrama con bits de extensión, como lo muestra la *Figura 1-9*, de modo que otras estaciones en la red verán que la red está ocupada y no intentaran la transmisión hasta después que la ráfaga esta completa.

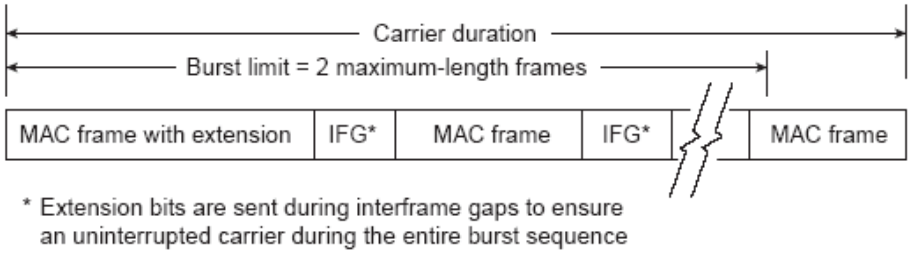



***Figura 1-9 Una secuencia Gigabit de ráfaga de trama***

Si la longitud de la primera trama es menor que el largo mínimo de trama, un campo de extensión se agrega para extender la longitud de la trama al valor indicado en la *Tabla 1-3*.
Las tramas subsecuentes en una secuencia en ráfaga de trama no necesitan campos de extensión, y una ráfaga de trama puede continuar tan larga como se pueda mientras el límite de la ráfaga no haya sido alcanzado. Si el límite de la ráfaga es alcanzado después de que una transmisión de trama ha iniciado, la transmisión se permite continuar hasta que se ha enviado la trama entera.

Los campos de extensión de la trama no están definidos, y el modo ráfaga no esta permitido para tasas de transmisión de 10 y 100 Mbps.

### 1.6.4 Transmisión Full-duplex

La operación full-duplex es una capacidad opcional de la MAC que permite simultáneamente dos vías de transmisión sobre links punto a punto. La transmisión full-duplex es funcionalmente mucho mas simple que la transmisión half-duplex porque no implica contención de los medios, ninguna colisión, ninguna necesidad de programar retransmisiones, y ninguna necesidad por bits de extensión al final de las tramas cortas. El resultado es no solamente más tiempo disponible para la transmisión, sino también el aumento al doble del ancho de banda del link porque cada link puede ahora soportar tasa llena, simultánea y dos vías de transmisión.

La transmisión suele comenzar tan pronto como las tramas están listas para enviarse. La única restricción es que debe haber un vacío mínimo entre tramas sucesivas, como se muestra en la *Figura 1-10*, y cada trama debe conformarse con los estándares del formato de trama de Ethernet.

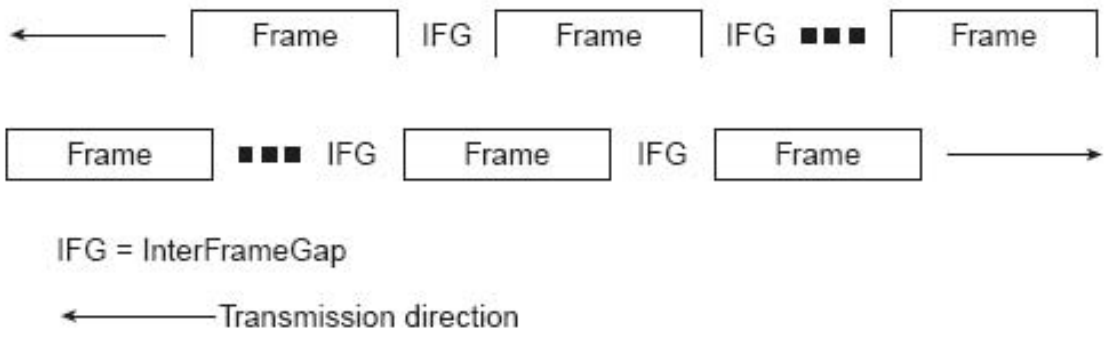



***Figura 1-10 La operación Full-duplex permite transmisiones de 2 vías simultáneamente en el mismo link***

### 1.6.5 Control de flujo

La operación full-duplex requiere implementación concurrente de la capacidad opcional de control de flujo que permite un nodo de recepción (como es un puerto de switch de red) que esta poniéndose congestionado para solicitar el nodo de envío (tal como un file server) para parar las tramas enviadas por un corto período de tiempo seleccionado. El control es MAC a MAC a través del uso de una trama de pausa que es automáticamente generada por la MAC receptora. Si la congestión es aliviada antes de que haya expirado la espera solicitada, una trama de un segundo con un valor cero de tiempo de espera puede ser enviada para solicitar la reanudación de la transmisión. Una descripción de la operación de control de flujo se muestra en la *Figura 1-11*.

La operación full-duplex y su compañía, la capacidad del control de flujo ambas son opciones para todas los MAC's de Ethernet y todas las tasas de transmisión. Ambas opciones están habilitadas en una base link a link, asumiendo que las capas físicas asociadas son también capaces de soportar la operación full-duplex.

Las tramas de pausa son identificadas como tramas de control MAC por un valor length/type (reservado) asignado y exclusivo. Ellos también son asignados a un valor de dirección reservado de destino para asegurarse que una trama de pausa entrante nunca sea reenviada a capas superiores del protocolo o a otros puertos en un switch.

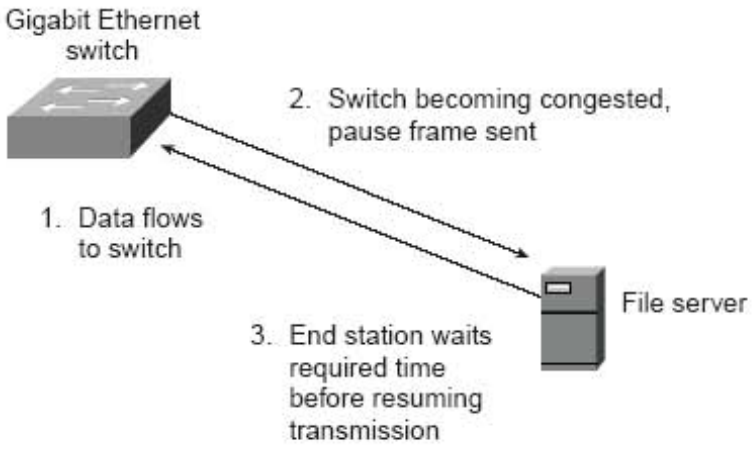



***Figura 1-11 Una descripción de la secuencia de control de flujo de la IEEE 802.3***

### 1.6.6 Recepción de trama

La recepción de trama es esencialmente igual para las operaciones half-duplex y full-duplex, excepto que las MAC's full-duplex deben tener buffers de trama separados y trayectorias de datos que permiten transmisión y recepción simultaneas.

La recepción de trama es el inverso de la transmisión. La dirección de destino de la trama recibida es checada y comparada contra la lista de dirección de estaciones (su dirección MAC, sus direcciones de grupo, y la dirección de difusión conocida como broadcast address) para determinar si la trama esta destinada para esa estación.
Si una dirección comparada es encontrada, se comprueba la longitud de la trama y el FCS recibido se compara al FCS que fue generado durante la recepción de la trama. Si la longitud de la trama esta bien y hay un FCS igual, el tipo de trama esta determinado por el tipo de contenido del campo Length/Type. La trama es entonces analizada y remitida a la capa superior apropiada.

### 1.6.7 La opción de etiquetado (Tagging) de VLAN

El etiquetado de VLAN es una opción del MAC que proporciona tres capacidades importantes no previamente disponible para los usuarios de red de Ethernet y administradores de red:

- Proporciona medios de apresurar tráfico de red en tiempo crítico fijando las prioridades de la transmisión para las tramas salientes.

- Permite que las estaciones sean agrupadas a grupos lógicos, para comunicarse a través de LANs múltiples como si estuvieran en una simple LAN. Puentes y switches filtran las direcciones de destino y reenvían tramas VLAN solo a puertos que sirven a la VLAN a la cual el tráfico pertenece.

- Simplifica el manejo de la red para sumar, mover, y cambiar más fácilmente al administrar.

Una trama VLAN etiquetada es simplemente una trama MAC de datos básica que ha tenido una cabecera de 4 bytes VLAN insertada entre el SA y los campos Length/Type, como se muestra en la *Figura 1-12*.

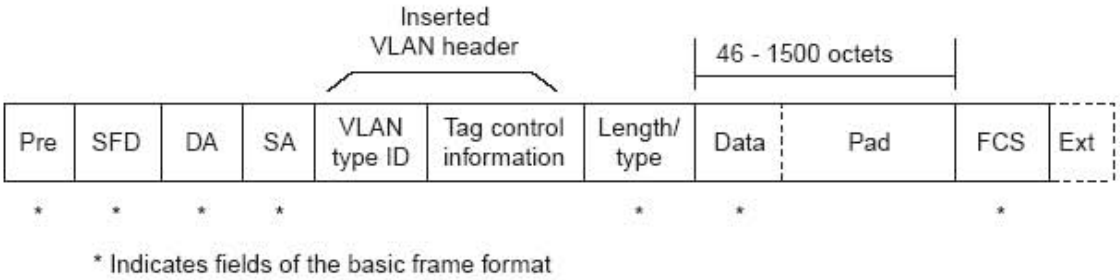



***Figura 1-12 Las tramas VLAN etiquetadas son identificadas cuando la MAC encuentra el valor del tipo LAN en el campo normal de localización Length/Type***

La cabecera VLAN consiste en dos campos:

- Un valor del tipo reservado de 2 bytes, indicando que la trama es una trama VLAN
- Un campo de dos bytes de control de etiquetado que contiene la prioridad de la transmisión (del 0 a 7, donde 7 es la mas alta) y un identificador de VLAN que identifica la VLAN particular sobre la cual la trama esta por ser enviada

La MAC receptora lee el valor del tipo reservado que está situado en la posición normal del campo Length/Type e interpreta la trama recibida como una trama de VLAN.

Entonces ocurre lo siguiente:

- Si la MAC está instalada en un puerto de switch, la trama es reenviada según su nivel de prioridad a todos los puertos que están asociados al identificador indicado de VLAN.
- Si la MAC está instalada en una estación final, esta remueve la cabecera VLAN de 4 bytes y procesa la trama de la misma manera que una trama de datos básica.

El etiquetado de VLAN requiere que todos los nodos de la red implicados con un grupo VLAN estén equipados con la opción de VLAN.

## 1.7 Las capas físicas de Ethernet

Debido a que los dispositivos Ethernet solo implementan las dos capas mas bajas de la pila del protocolo OSI, ellos son típicamente implementados como tarjetas de interfaz de red (NICs, Network Interface Cards) que se conectan en la tarjeta madre del aparato huésped. Las diferentes NICs son identificadas por un nombre de producto de tres partes que esta basado en los atributos de la capa física.

La convención de nombres es una concatenación de tres términos que indican la tasa de transmisión, el método de transmisión, y la codificación del tipo/señal del medio. Por ejemplo, considérese esto:

- 10BaseT = 10 Mbps, banda base, sobre 2 cables de par trenzado
- 100Base-T2 = 100 Mbps, banda base, sobre 2 cables de par trenzado
- 100Base-T4 = 100 Mbps, banda base, sobre 4 cables de par trenzado
- 1000Base-LX = 100 Mbps, banda base, onda larga sobre cable de fibra óptica

Una pregunta se presenta a veces en cuanto a por que el término medio parece siempre ser "Base".
Las versiones tempranas del protocolo también se permitían para transmisión de banda ancha (por ejemplo, 10Broad), pero las implementaciones de banda ancha no fueron exitosas en el mercado. Todas las implementaciones actuales de Ethernet utilizan la transmisión de banda base.

### 1.7.1 Codificación de la señal de transmisión

En la transmisión de banda base, la información de la trama es directamente impresa sobre el link como una secuencia de pulsos o símbolos de datos que son típicamente atenuados (reducido de tamaño) y distorsionados (cambiados de forma) antes de que alcancen el otro final del link. La tarea del receptor es detectar cada pulso cuando este llega y entonces extraer su valor correcto antes de transferir la información reconstruida a la MAC de recepción.

Los filtros y los circuitos de forma de pulso pueden ayudar a restaurar el tamaño y la forma de las formas de onda recibidas, pero las medidas adicionales deben ser tomadas para asegurarse que las señales recibidas están muestreadas en el tiempo correcto en el período del pulso y en la misma tasa que el reloj de transmisión:

- El reloj receptor debe ser recuperado de la secuencia de datos entrante para permitir que la capa física receptora se sincronice con los pulsos entrantes.
- Las medidas compensadoras deben ser tomadas para un efecto conocido como línea base vaga (baseline wander).

La recuperación del reloj requiere niveles de transición en la señal entrante para identificar y sincronizar los límites del pulso. Los 1s y los 0s alternados del preámbulo de la trama fueron diseñados para indicar que una trama estaba llegando y para ayudar en la recuperación del reloj. Sin embargo, los relojes recuperados pueden apilarse y posiblemente perder sincronización si los niveles del pulso permanecen constantes y no hay transiciones a detectar (por ejemplo, durante cadenas largas de 0s).

La línea base vaga resulta porque los links Ethernet son acoplados a los transceptores de CA y porque el acoplamiento de CA es incapaz de mantener niveles de voltaje por más de un corto tiempo. Como resultado, los pulsos transmitidos están distorsionados por un efecto de la inclinación similar al ejemplo exagerado mostrado en la *Figura 1-13*. En cadenas largas de 1s o de 0s, la inclinación puede llegar a ser tan severa que el nivel de voltaje pasa a través del umbral de decisión (Decision threshold), resultando en valores muestreados erróneos para los pulsos afectados.

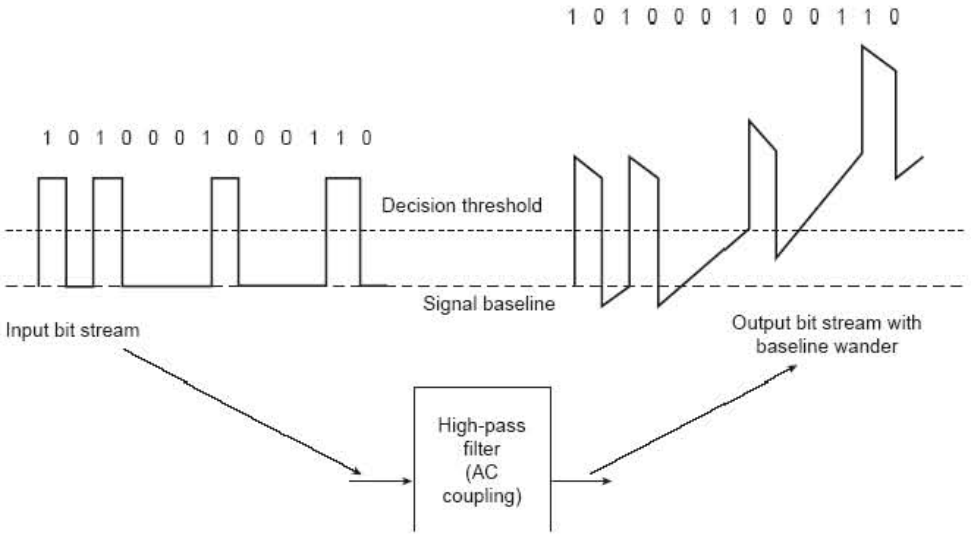



***Figura 1-13 Un ejemplo del concepto de línea base vaga (Baseline Wander)***

Afortunadamente, codificar la señal de salida antes de la transmisión puede reducir significativamente el efecto de ambos problemas, así como disminuye la posibilidad de errores en la transmisión.
En las primeras implementaciones de Ethernet, incluyendo la 10BaseT, todas utilizaron el método de codificación Manchester, mostrado en la *Figura 1-14*. Cada pulso es identificado claramente por la dirección de la transición de la mitad del pulso más bien que por su valor llano muestreado.

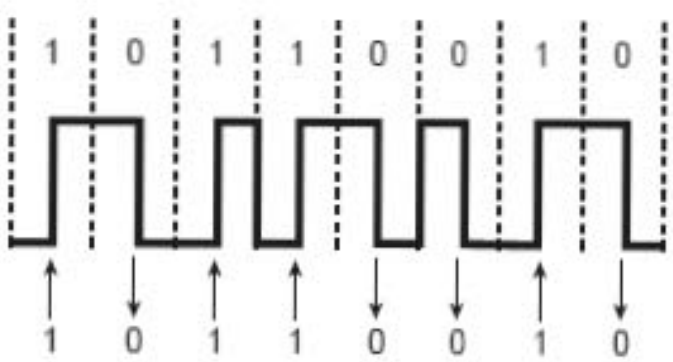



***Figura 1-14 Codificación Manchester basada en transición binaria***

Desafortunadamente, la codificación Manchester introduce algunos problemas difíciles relacionados a la frecuencia que lo hacen inadecuado para usarlo en altas tasas de datos.

Todas las versiones de Ethernet subsecuentes a 10BaseT usan diversos procedimientos de codificación que incluyen algunas o todas las técnicas siguientes:

- **Usando datos revueltos (Data scrambling)** — Un procedimiento que revuelve los bits en cada byte en una manera ordenada (y recuperable). Algunos 0s se cambian a 1s, algunos 1s se cambian a 0s, y algunos bits se dejan igual. El resultado es reducir la longitud de bits del mismo valor, incrementando la densidad de transición, y facilitando la recuperación del reloj.

- **Expandiendo el espacio de código** — Una técnica que permite asignar por separado códigos para datos y símbolos de control (como son delimitadores de inicio y fin de flujo, bits de extensión, etcétera) y que asiste en la detección de error de transmisión.

- **Usando códigos de reenvío de error-corrección** — Una codificación en la que información redundante se suma a la secuencia de datos transmitida, así algunos tipos de errores de transmisión pueden ser corregidos durante la recepción de la trama.

**Nota**
Códigos de reenvió de error-corrección son usados en 1000Base-T para lograr una reducción efectiva en la tasa de error de bits. El protocolo Ethernet limita el manejo de errores de bit en la trama recibida. La recuperación de las tramas recibidas con errores incorregibles o tramas perdidas es responsabilidad de las capas más altas en la pila del protocolo.

### 1.7.2 La relación de la capa física 802.3 al modelo de referencia ISO

Aunque el modelo lógico específico de la capa física puede variar de versión a versión, todas la NICs Ethernet generalmente son similares al modelo genérico mostrado en la *Figura 1-15*.

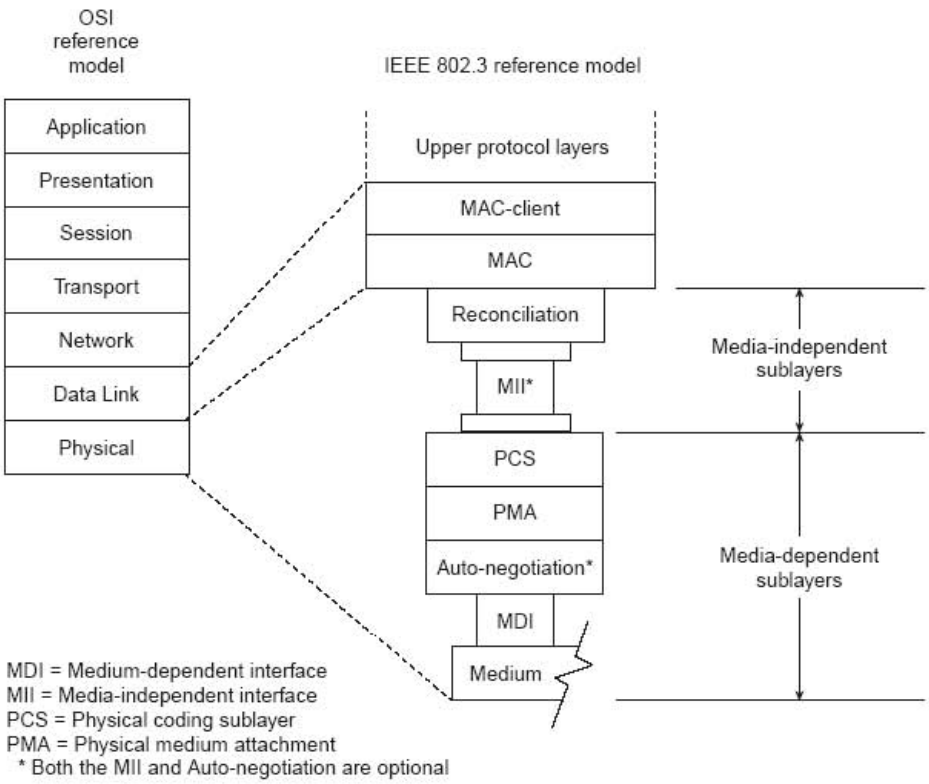



***Figura 1-15 El modelo genérico de referencia de Capa física Ethernet***

La capa física para cada tasa de transmisión esta dividida en subcapas que son independientes del tipo de medio particular y subcapas que son específicas a la codificación de la señal o tipo de medio.

- La subcapa de reconciliación y la interfaz opcional independiente del medio (MII en Ethernet a 10 Mbps y 100 Mbps, GMII en Gigabit Ethernet) proporcionan conexión lógica entre la MAC y los diversos tipos de capas dependientes del medio. El MII y los GMII son definidos con transmisión separada y reciben trayectorias de datos que son implementaciones de bits en serie para 10 Mbps, serie pequeña (4 bits de anchura) para las implementaciones de 100 Mbps, y serie de bytes (con 8 bits de ancho) para las implementaciones a 1000 Mbps. Las interfaces independientes del medio y la subcapa de reconciliación son comunes para sus respectivas tasas de transmisión y son configuradas para la operación full-duplex en 10BaseT y todas las versiones subsecuentes de Ethernet.
- La subcapa física de codificación dependiente del medio (PCS, Physical Coding Sublayer) proporciona la lógica para la codificación, multiplexación y la sincronización del flujo del símbolo saliente así como la alineación correcta del código, demultiplexación, y el decodificado de los datos entrantes.
- La subcapa física de medio agregado (PMA, Physical Médium Attachment) contiene las señales transmisora y receptora, así como la lógica de recuperación de reloj para los flujos de datos recibidos.
- La interfaz dependiente del medio (MDI, Medium Dependent Interface) es el conector del cable entre los transceptores (transmisores-receptores) y el link.
- La subcapa de autonegociación permite a las NICs en cada final del link intercambiar información acerca de sus capacidades individuales, y entonces negociar y seleccionar el modo operacional más favorable que ambos sean capaces de soportar. La autonegociación es opcional en las implementaciones Ethernet tempranas y es obligatoria en las últimas versiones.

Dependiendo de qué tipo de codificación de señal es usada y cómo los links son configurados, las PC y PMA pueden o no ser capaces de soportar la operación full-duplex.

### 1.7.3 Ethernet a 10 Mbps — 10Base-T

La 10Base-T proporciona comunicación con codificación Manchester de 10 Mbps con bit serial sobre dos cables no blindados de par trenzado. Aunque el estándar fue diseñado para soportar transmisión sobre cable telefónico común, la configuración más típica de link es usar dos pares de 4 de un cable Categoría 3 o 5, terminado en cada NIC con un conector RJ-45 (el MDI), como se muestra en la *Figura 1-16*. Porque cada par activo esta configurado como un simple link en donde la transmisión es solo en una dirección, las capas físicas 10BaseT pueden soportar o la operación half-duplex o full-duplex.

Aunque la 10BaseT puede ser considerada esencialmente obsoleta en algunos círculos, se incluye aquí porque todavía hay muchas redes Ethernet 10BaseT, y porque la operación full-duplex ha dado a 10BaseT una vida extendida.

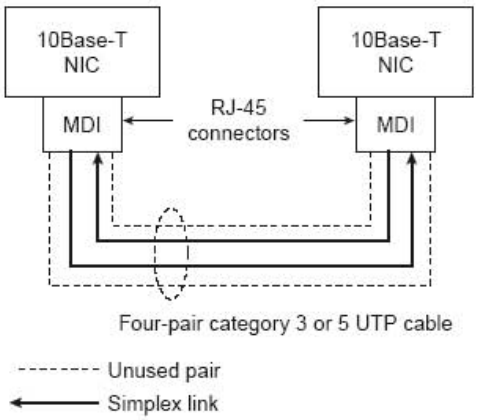



***Figura 1-16 El típico link 10Base-T es un cable UTP de 4 pares en el que 2 pares no son usados***

La 10BaseT fue también la primera versión de Ethernet para incluir una prueba de integridad del link (acoplamiento) para determinar la salud del link. Inmediatamente después de la actualización, el PMA transmite un pulso normal de acoplamiento (NLP Normal Pulse Link) para decir al NIC en el otro extremo del link que este NIC quiere establecer una conexión activa de enlace:

- Si el NIC en el otro extremo del link también esta accionado, responde con su propio NLP
- Si el NIC en el otro extremo del link no esta accionado, éste NIC continúa enviando un NLP alrededor de 16 *ms* hasta que recibe una respuesta.

El link es activado solo después de que ambas NICs son capaces de intercambiar NLP's validas.

### 1.7.4 Fast Ethernet — 100 Mbps

El aumento de la tasa de transmisión de Ethernet en un factor de 10 sobre 10BaseT no fue una tarea simple, y el esfuerzo dio lugar al desarrollo de tres estándares separados de la capa física para 100 Mbps sobre cable UTP: 100Base-TX y 100Base-T4 en 1995, y 100Base-T2 en 1997. Cada uno fue definido con diversos requisitos de codificación y un diverso sistema de subcapas dependientes del medio, aunque hay un cierto traslape en el cableado del link.

La *Tabla 1-4* compara las características de la capa física de 10BaseT y las varias versiones de 100Base.

Aunque no todas las tres versiones de 100 Mbps fueron exitosas en el mercado, las tres han sido discutidas en la literatura, y las tres impactaron los diseños futuros. Como tal, es importante considerar las tres que aquí se muestran.

| Versión Ethernet | Tasa[1] de símbolo transmitido | Codificación | Cableado | Operación Full-Duplex |
|---|---|---|---|---|
| 10Base-T | 10 MBd | Manchester | 2 pares de UTP Categoría 3 o mayor | Soportada |
| 100Base- TX | 125 MBd | 4B/5B | 2 pares de UTP Categoría 5 o STP Tipo 1 | Soportada |
| 100Base-T4 | 33 MBd | 8B/6T | 4 pares de UTP Categoría 3 o mayor | No soportada |
| 100Base-T2 | 25 MBd | PAM5x5 | 2 pares de UTP Categoría 3 o mayor | Soportada |

[1] Un Baudio= Un símbolo transmitido por segundo, donde el símbolo transmitido puede contener el valor equivalente de uno o mas bits binarios

***Tabla 1-4 Resumen de las características de la capa física 100Base-T***

### 1.7.5 100Base-X

100Base-X fue diseñada para soportar la transmisión o sobre dos pares cable de cobre Categoría 5 UTP o sobre dos hilos de fibra óptica. Aunque la codificación, el descifrado, y los procedimientos de recuperación de reloj son iguales para ambos medios, la transmisión de la señal es distinta — pulsos eléctricos en el cable de cobre y pulsos de luz en la fibra óptica.
Los transmisores-receptores de señal que fueron incluidos como parte de la función PMA en el modelo lógico genérico de la *Figura 1-15* fueron redefinidos como subcapas separadas dependientes del medio (PMD Physical Media-Dependent) mostradas en la *Figura 1-17*.

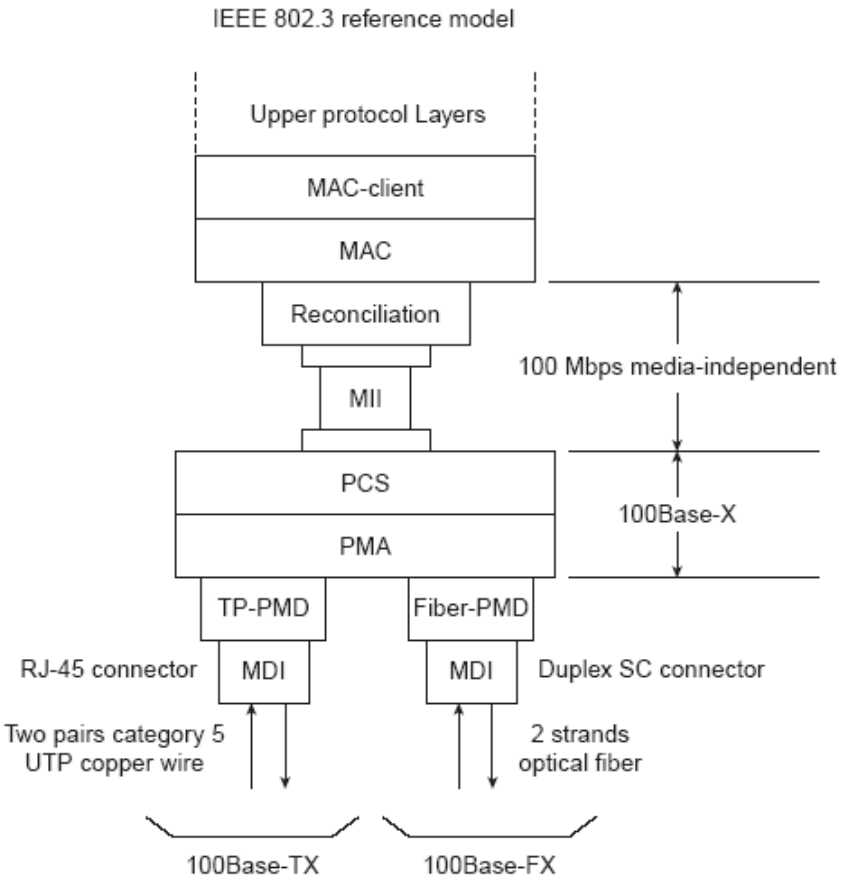



***Figura 1-17 El modelo lógico 100Base-X***

El procedimiento de codificación 100Base-X esta basado en los primeros estándares de fibra óptica FDDI dependientes del medio físico y los estándares de señal dependientes del medio físico para par trenzado de cobre FDDI/CDDI desarrollados por la ISO y la ANSI. La subcapa física dependiente del medio 100Base-TX (TP-PMD) fue puesta en ejecución con transceptores y conectores RJ-45; la fibra PMD fue puesta en marcha con FDDI y transmisores-receptores ópticos del FDDI y un conector de interfaz de fibra de bajo costo (Low Cost Fiber Interface Connector) comúnmente llamado Conector SC Duplex.

El procedimiento de codificación 4B/5B es igual al procedimiento de codificación usado por FDDI, con adaptaciones de menor importancia para acomodar el control de trama Ethernet. Cada trozo de datos de 4 bits (que representan la mitad de un byte de datos) es mapeado a un grupo de código binario de 5 bits que es transmitido sobre un link de bits del tipo serial.

El espacio de código expandido proporcionado por los 32 grupos de código de 5 bits permite asignar separadamente como sigue:

- Los 16 valores posibles en un trozo de datos de 4 bits (16 grupos de código).
- Cuatro grupos de código de control que son transmitidos como pares de grupos de código para indicar el inicio del delimitador de flujo (SSD Start-of-Stream Delimiter) y el delimitador del fin de flujo (ESD End-of-Stream Delimiter). Cada trama MAC es “encapsulada" para marcar el principio y el final de la trama. El primer byte del preámbulo es reemplazado con un par códigos de grupo SSD que precisamente identifica las fronteras del grupo de códigos de la trama. El par de grupos de código ESD se suma después del campo FCS de la trama.
- Un grupo especial de códigos IDLE que es continuamente enviado durante vacíos intertramas para mantener sincronización continua entre las NICs y cada link final. El recibo de IDLE es interpretado como que el link esta quieto.
- Once grupos de código inválidos que no son transmitidos intencionalmente por un NIC (aunque uno es usado por un repetidor para propagar errores recibidos). La recepción de cualquier grupo de códigos inválido causará que la trama entrante sea tratada como una trama invalida.

La *Figura 1-18* muestra cómo la trama MAC se encapsula antes de ser transmitida como un flujo de grupos de código 100Base-X.

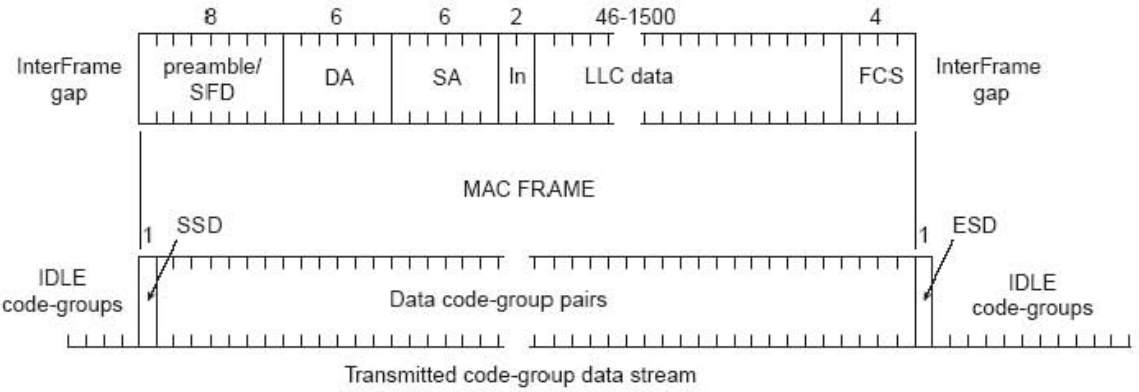



***Figura 1-18 El flujo de Grupos de código 100Base-X con Encapsulación de Trama***

100Base-TX transmite y recibe en los mismos pares de links y usa las mismas asignaciones de pines en el MDI como en 10Base-T. Para 100Base-TX y 100Base-FX ambas soportan la transmisión half-duplex y full-duplex.

### 1.7.6 100Base-T4

100Base-T4 fue desarrollado para permitir a las redes 10BaseT ser actualizadas a una operación a 100 Mbps sin cambiar los cables existentes Categoría 3 UTP de cuatro pares para ser substituidos por los más nuevos de Categoría 5. Dos de los cuatro pares son configurados para operación half-duplex y pueden soportar la transmisión en cualquier dirección, pero solamente en una dirección a la vez. Los otros dos pares se configuran como pares simples dedicados a la transmisión solo en una dirección.
La transmisión de trama usa ambos pares half-duplex, más el par simple que es apropiado para la dirección de la transmisión, como es mostrado en la *Figura 1-19*. El par simple para la dirección opuesta proporciona sentido a la portadora y detección de colisión. La operación full-duplex no es soportada en 100Base-T4.

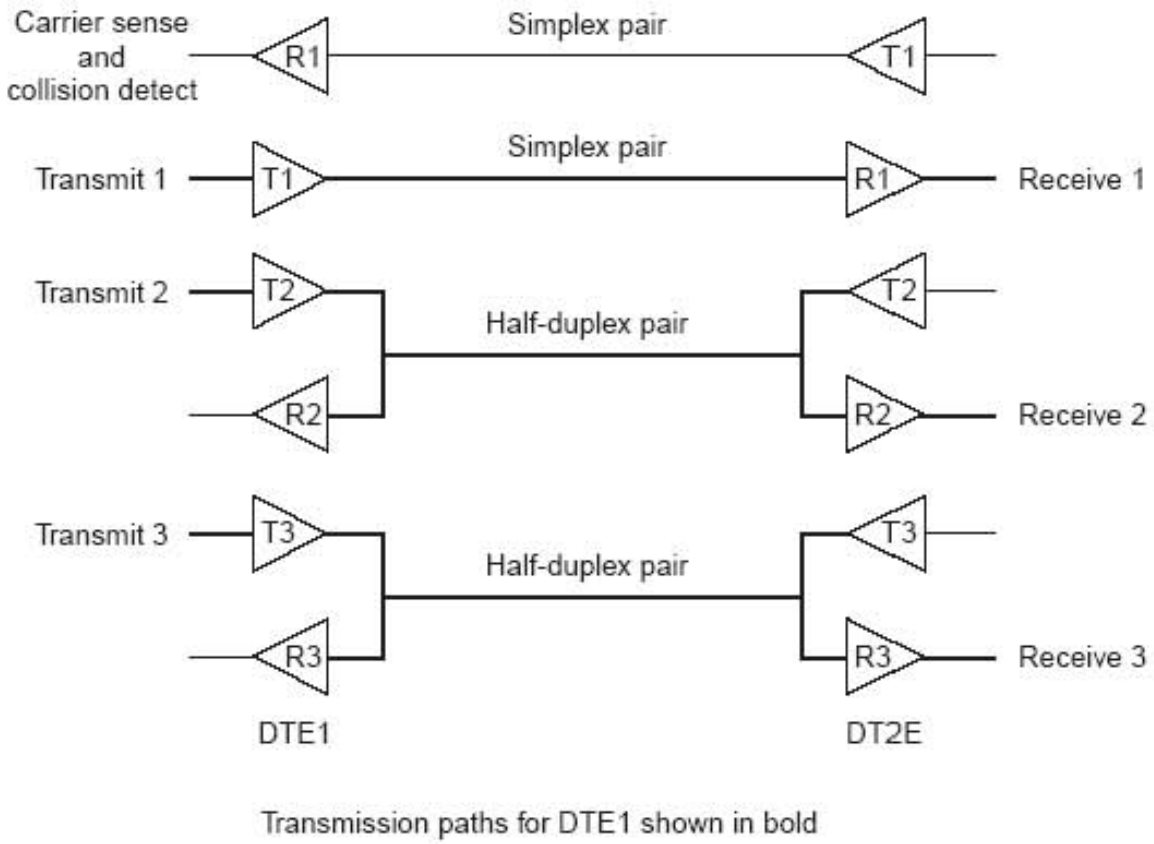



***Figura 1-19 Uso de los pares de cable 100Base-T4 durante la transmisión de trama***

100Base-T4 utiliza un esquema de codificación 8B6T en el cual cada byte de 8 bits binarios es mapeado en un patrón de símbolos de seises ternarios (tres niveles: +1, 0, –1) conocidos como grupo de códigos 6T. Grupos de código separados 6T se utilizan para IDLE y para grupos de código de control que son necesarios para la transmisión de la trama. Un IDLE recibido en el par dedicado para recepción indica que el link esta quieto.

Durante la transmisión de trama, grupos de códigos de datos 6T son transmitidos en una secuencia retardada tipo round-robin sobre los tres pares de cables de transmisión, como se muestra en la *Figura 1-20*. Cada trama es encapsulada con grupos de código 6T de inicio de flujo y fin de paquete (start-of-stream and end-of-packet) y ambos marcan el inicio y el final de la trama, y el inicio y el fin del flujo de grupos de código 6T en cada par de cables. La recepción de un grupo de código no IDLE sobre el par de cables dedicado a la recepción en cualquier momento antes de que expire la ventana de colisión indica que una colisión ha ocurrido.

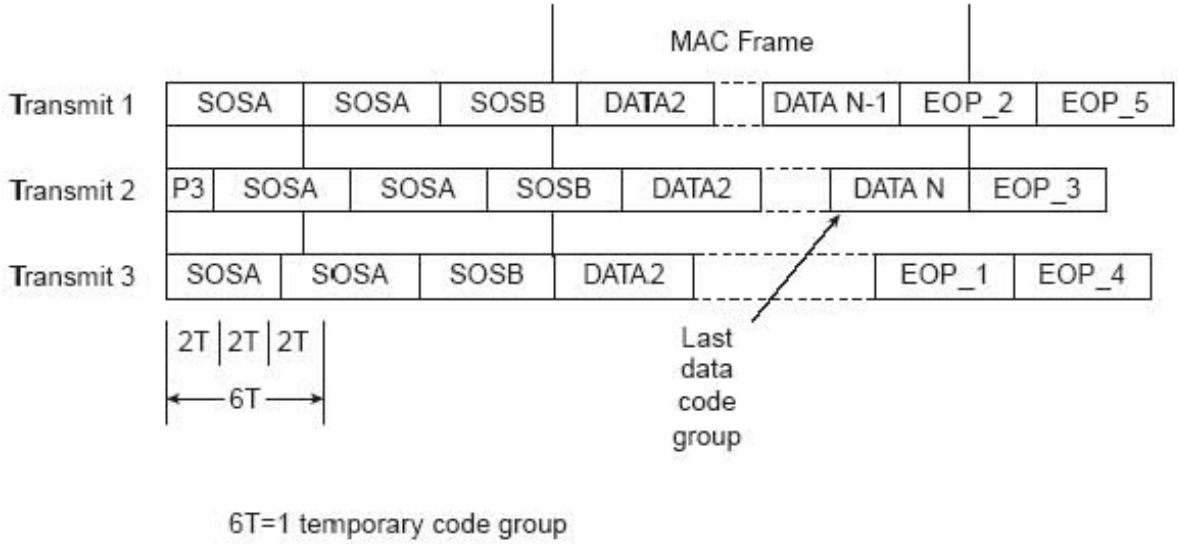



***Figura 1-20 La secuencia de transmisión de trama en 100Base-T4***

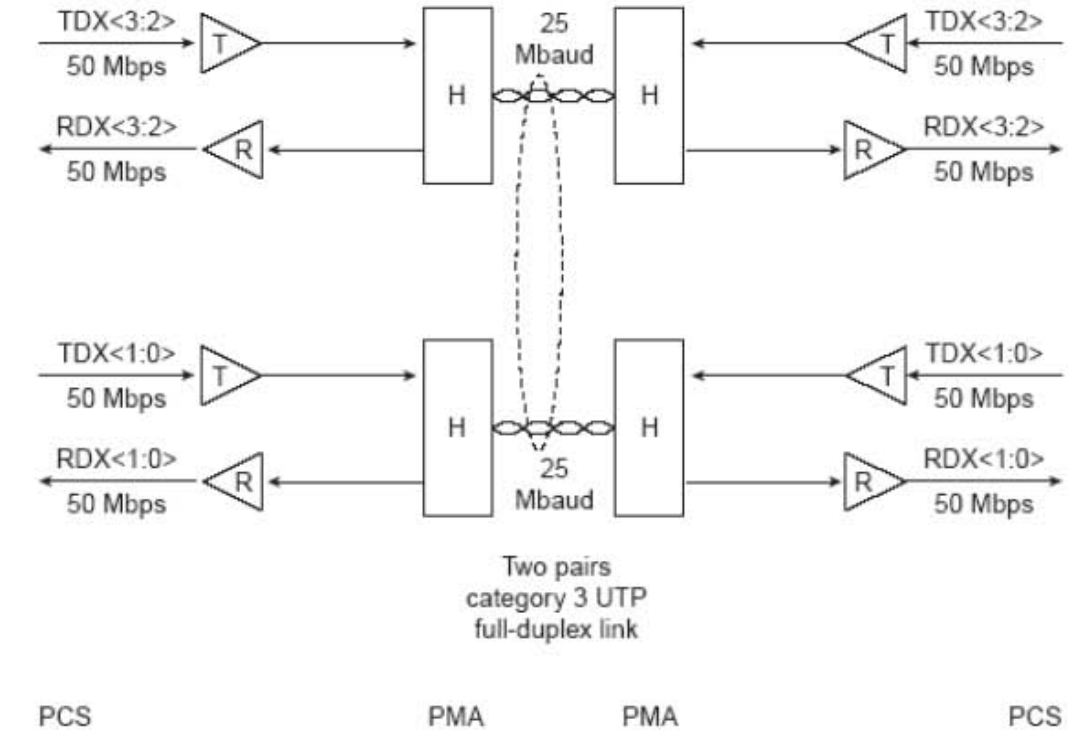
### 1.7.7 100Base-T2

La especificación 100Base-T2 fue desarrollada como una mejor alternativa para actualizar redes con cableado instalado de Categoría 3 que fue siendo suministrada por 100Base-T4. Dos nuevas metas importantes fueron definidas:

- Para proporcionar la comunicación sobre dos pares de Categoría 3 o un cable mejor
- Para apoyar la operación half-duplex y full-duplex

100Base-T2 utiliza un procedimiento de transmisión de señal diferente a cualquier implementación previa Ethernet con pares de cable. En vez de usar dos simples links para formar un link full-duplex, el método de transmisión de banda base 100Base-T2 dual-duplex envía símbolos codificados simultáneamente en ambas direcciones en ambos pares de cable, como se muestra en la *Figura 1-21*. El término "TDX<3:2 >" indica los 2 bits más significativos del trozo antes de la codificación y de la transmisión. "RDX<3:2 >" indica los mismos 2 trozos después de la recepción y decodificación.

La transmisión de banda base Dual-duplex requiere que las NICs en cada final del link estén operando en un modo de tiempo en bucle maestro-esclavo. Qué NIC será maestra y cuál será esclava esta determinado por la autonegociación durante la iniciación del link. Cuando el link es operacional, la sincronización se basa en el reloj de transmisión interno de la NIC maestra. La NIC esclava utiliza el reloj recuperado para transmitir y recibir operaciones, según lo mostrado en la *Figura 1-22*.
Cada trama transmitida es encapsulada, y la sincronización del link es mantenida con un flujo continuo de símbolos IDLE durante los vacíos intertramas.




H = Hybrid canceller transceiver
T = Transmit encoder
R = Receive decoder
Two PAM5 code symbols = One nibble

***Figura 1-21 Topología del link en 100Base-T2***

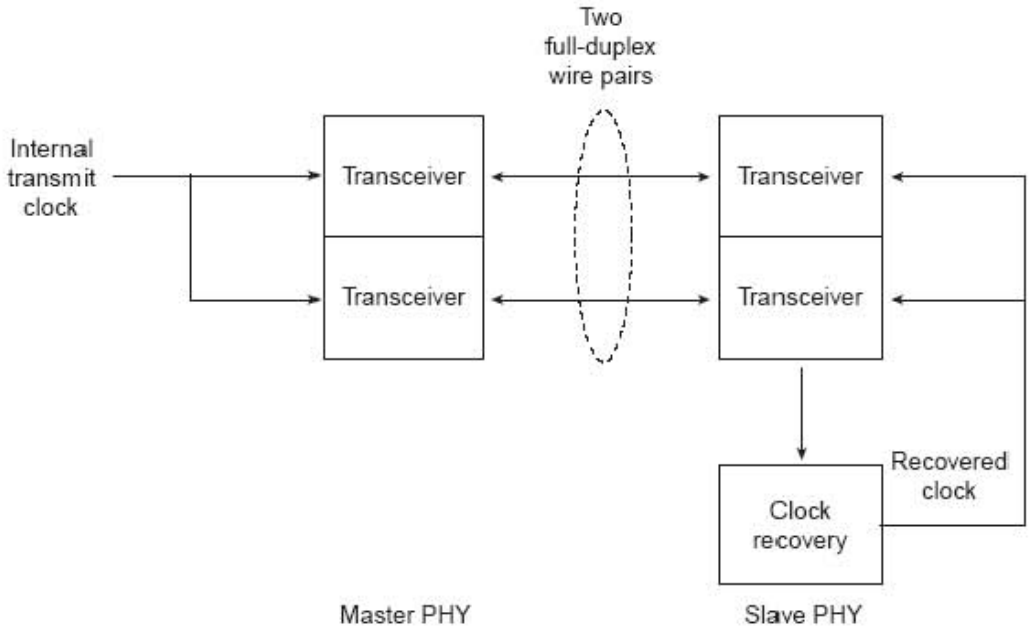



***Figura 1-22 Configuración del bucle de tiempo en 100Base-T2***

El proceso de codificación 100Base-T2 primero revuelve los trozos de datos de trama en una secuencia de datos aleatoria. Ésta entonces mapea los 2 bits mas altos y los 2 bits mas bajos de cada trozo en dos niveles de cinco (+2, +1, 0, –1, –2) símbolos de pulsos modulados en amplitud (PAM) que son simultáneamente transmitidos sobre dos pares de cables (PAM5x5). Diversos procedimientos de revolvimiento para las transmisiones maestro-esclavo aseguran que las secuencias de datos que viajan en direcciones opuestas en el mismo par de alambres no estén coordinadas.
La recepción de la señal es esencialmente al revés de la transmisión de la señal. Ya que la señal en cada par de alambres en el MDI es la suma de la señal transmitida y la señal recibida, cada receptor resta los símbolos transmitidos desde la señal recibida al MDI para recobrar los símbolos en la secuencia de datos entrante. El par entrante de símbolos es entonces descifrada, se decodifica, y es reconstituida como datos para la transferencia a la MAC.

### 1.7.8 1000 Mbps — Gigabit Ethernet

El desarrollo de los estándares Gigabit Ethernet resulto en 2 especificaciones primarias: 1000Base-T para cable de cobre UTP y 1000Base-X para cable de cobre STP, así como para fibra óptica sencilla y fibra óptica multimodo (ver *Figura 1-23*).

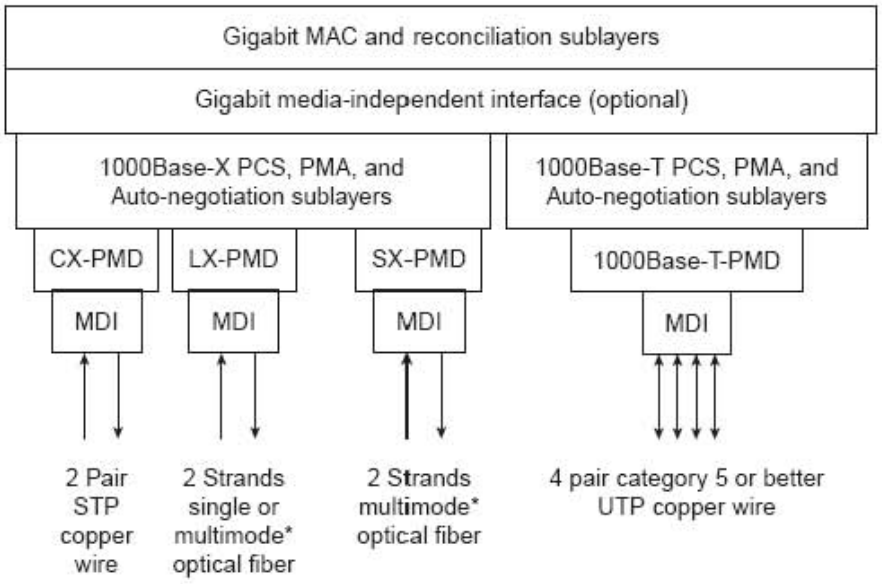



***Figura 1-23 Variaciones Gigabit Ethernet***

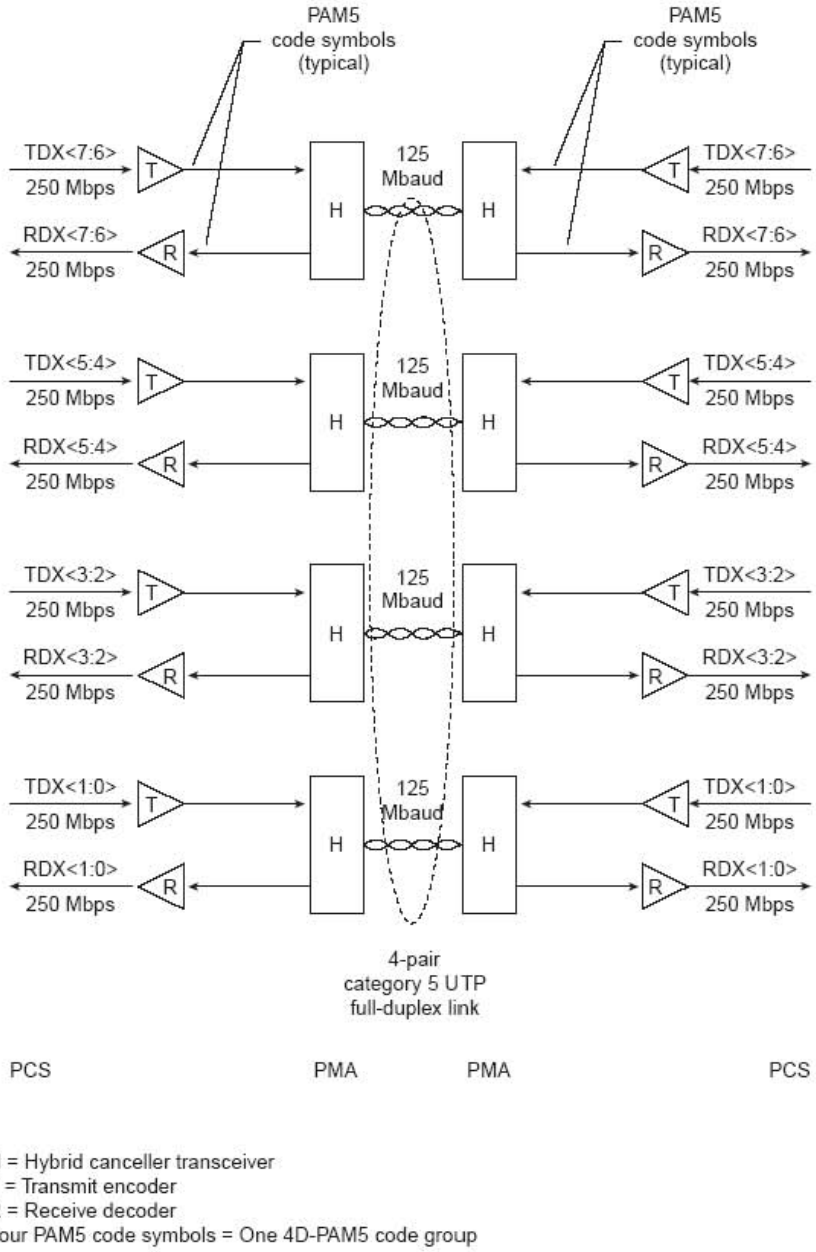
### 1.7.9 1000Base-T

Ethernet 1000Base-T proporciona transmisión full-duplex sobre cables UTP de cuatro pares Categoría 5 o mejor. 1000Base-T se basa en gran parte en los resultados y los acercamientos de diseño que dirigía el desarrollo de las implementaciones Fast Ethernet en la capa física:

- 100Base-TX probó que las corrientes binarias de símbolos podrían ser transmitidas con éxito sobre cable UTP Categoría 5 a 125 MBd.
- 100Base-T4 proporcionó una comprensión básica de los problemas relacionados al envío de señales multinivel sobre cuatro pares de cables.
- 100Base-T2 probó que la codificación PAM5 junto al procesamiento digital de señal, podría manejar ambas secuencias de flujo de datos simultáneamente y problemas potenciales de interferencia (crosstalk) resultado de señales externas o pares adyacentes de cable.

1000Base-T revuelve cada byte en la trama MAC para seleccionar al azar la secuencia de bits antes de que sea encogida usando un 4-D, la codificación de “Corrección de error de reenvío Trellis de 8 estados” (FEC, 8-State Trellis Forward Error Correction) en la cual cuatro símbolos PAM5 son enviados al mismo tiempo sobre cuatro pares de cable. Cuatro de los cinco niveles en cada símbolo PAM5 representa 2 bits en los bytes de datos.
El quinto nivel es usado para la codificación FEC, que mejora la recuperación de símbolos en la presencia de ruido e interferencia. Los revolvedores separados para los PHYs maestro y esclavo crean esencialmente secuencias de datos sin correlación entre las dos secuencias de símbolos opuestos que viajan en cada par de cables.

La topología del link 1000Base-T se muestra en la *Figura 1-24*. El término "TDX<7:6 >" indica los 2 bits más significativos en el byte de datos antes de la codificación y transmisión. "RDX<7:6 >" indica los mismos 2 bits después de recibir y descifrar.




H = Hybrid canceller transceiver
T = Transmit encoder
R = Receive decoder
Four PAM5 code symbols = One 4D-PAM5 code group

***Figura 1-24 Topología de acoplamiento en 1000Base-T***

La recuperación del reloj y los procedimientos de tiempo de bucle maestro/esclavo son esencialmente iguales a las usadas en 1000Base-T (ver *Figura 1-25*). Cual NIC será el maestro (típicamente la NIC en un nodo de red intermedio de un multipuerto) y cuál será esclavo se determina durante el autonegociación.

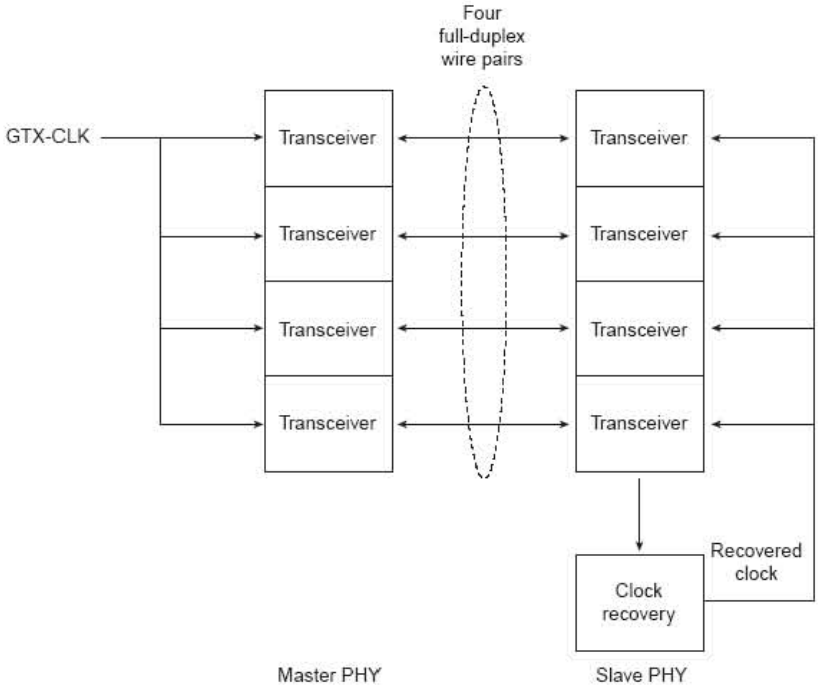



***Figura 1-25 Configuración del bucle de tiempo Maestro/Esclavo en 1000Base-T***

Cada trama transmitida se encapsula con los delimitadores de inicio de ráfaga y de fin de ráfaga, y la sincronización del bucle es mantenida por ráfagas continuas de símbolos IDLE enviados en cada par de cable durante los vacíos intertrama. 1000Base-T soporta las operaciones half-duplex y full-duplex.

### 1.7.10 1000Base-X

Las tres versiones 1000Base-X soportan la transmisión binaria full-duplex a 1250 Mbps sobre dos hilos de fibra óptica o dos pares de alambre de cobre STP, según lo mostrado en la *Figura 1-26*.
La codificación de la transmisión se basa en el esquema de codificación **Fiber Channel 8B/10B** de **ANSI**. Cada byte de 8 bits es mapeado en un grupo de códigos de 10 bits para transmisión serial. Como en versiones anteriores de Ethernet, cada trama de datos es encapsulada en la capa física antes de la transmisión, y la sincronización del link es mantenida enviando ráfagas continuas de grupos de código IDLE durante los vacíos intertramas. Todas las capas físicas 1000Base-X soportan la operación half-duplex y full-duplex.

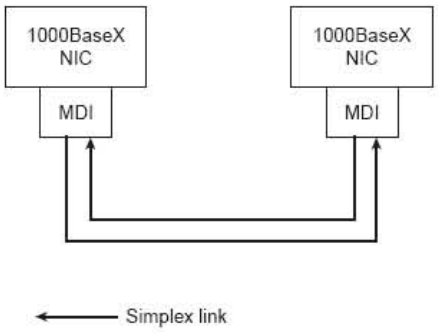



***Figura 1-26 Configuración del Link en 1000Base-X***

Las diferencias principales entre las versiones 1000Base-X son los medios de acoplamiento y los conectores que las versiones particulares soportaran y en el caso de medios ópticos, la longitud de onda de la señal óptica (ver *Tabla 1-5*).

| **Configuración de link** | **1000Base-CX** | **1000Base-SX (longitud de onda 850 nm)** | **1000Base-LX (longitud de onda 1300 nm)** |
|---|---|---|---|
| Cobre STP de 150 Ω | Soportada | No soportada | No soportada |
| Fibra[1] óptica multimodo de 125/62.5 µm | No soportada | Soportada | Soportada |
| Fibra óptica multimodo de 125/50 µm | No soportada | Soportada | Soportada |
| Fibra óptica monomodo de 125/10 µm | No soportada | No soportada | Soportada |
| Conectores permitidos | IEC estilo 1 ó Fiber Channel estilo 2 | SFF MT-RJ ó Duplex SC | SFF MT-RJ ó Duplex SC |

[1] La especificación 125/62.5 µm se refiere a los diámetros del revestimiento y el núcleo de la fibra

***Tabla 1-5 Soporte de los links de configuración 1000Base-X***

### 1.7.11 Cableado de red — Requerimientos para links cruzados (Crossover Links)

La compatibilidad de links requiere que los transmisores en cada fin del link estén conectados a los receptores en el otro extremo del link. Debido a que los conectores de cable en ambos extremos del link se afinan al mismo tiempo los conductores deben cruzarse en un punto para asegurar que las salidas del transmisor están conectadas siempre a las entradas del receptor.

Desafortunadamente, cuando este requisito vino primero en el desarrollo de 10BaseT, IEEE 802.3 eligió no hacer una regla clara de si el crossover debería ser implementado en el cable como se muestra en la *Figura 1-27a* o si debería ser implementado internamente como se muestra en la *Figura 1-27b*.

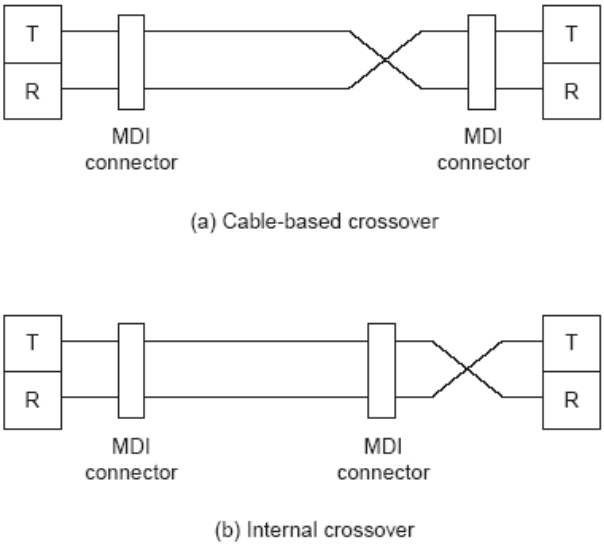



***Figura 1-27 Vías alternativas para implementar el requerimiento de link crossover***

En su lugar, IEEE 802.3 definió dos reglas e hizo dos recomendaciones:

- Debe haber un número impar de crossovers en todos los links multiconductor.
- Si un PMD esta equipado con un crossover interno, su MDI debe ser etiquetado claramente con el símbolo gráfico X.
- La implementación de una función de crossover interno es opcional.
- Cuando un DTE está conectado a un repetidor (hub) o a un switch de puerto (DCE), se recomienda que el crossover este implementado dentro del puerto DCE.

El resultado eventual fue que los puertos en la mayoría de los DCEs fueron equipados con PMDs que contenían circuitería interna crossover y que los DTEs tenían PMDs sin crossovers internos. Esto condujo a la “Regla de instalación” de facto siguiente:

- Usar un cable straight-through (directo) al conectar un DTE con un DCE. Usar un cable cruzado al conectar un DTE a un DTE o un DCE con un DCE.

Desafortunadamente, dicha regla no se aplica a todas las versiones de Ethernet que han sido subsecuentes a 10BaseT. Lo que es cierto es lo siguiente:

- Todos los sistemas basados en fibras usan cables que tienen el crossover implementado dentro del cable de fibra.
- Todos los sistemas 100Base que usan links de par trenzado usan las mismas reglas y recomendaciones que los 10BaseT.
- Los NICs 1000Base-T pueden implementar una opción seleccionable de crossover interno que puede ser negociado y habilitado durante la negociación. Cuando la opción seleccionable de crossover no esta implementada, las reglas y recomendaciones 10Base-T se aplican.

## 1.8 Consideraciones del Sistema

Dado todas las opciones discutidas previamente, puede parecer que no sería problema el actualizar una red existente o planear una nueva red. El problema es doble. No todas las opciones son razonables para todas las redes, y no todas las versiones de Ethernet y opciones están disponibles en el mercado, aun pensando que ellas han sido especificadas en el estándar.

### 1.8.1 Seleccionando componentes basados en UTP y Categoría del medio físico

Ahora, debe ser obvio que los NICs basados en UTP están disponibles para implementaciones de 10 Mbps, 100 Mbps y 1000 Mbps. La opción es relativamente simple para ambas operaciones a 10 Mbps y 1000 Mbps: 10BaseT y 1000Base-T. Desde las discusiones anteriores, sin embargo, esto no parece ser así de simple para implementaciones a 100 Mbps.

Aunque tres NICs basadas en UTP son definidas para 100 Mbps, el mercado ha limitado de forma efectiva la opción a solo 100Base-TX, la cual llegó a estar ampliamente disponible durante la primera mitad de 1995:

- Para el momento en que los primeros productos 100Base-T4 aparecieron en el mercado, 100Base-TX fue bien atrincherada, y el desarrollo de la opción full-duplex, la cual 100Base-T4 no podía soportar, iba por buen curso.
- El estándar 100Base-T2 no fue aprobado hasta la primavera de 1997, demasiado tarde para interesar al mercado. Como resultado, los productos 100Base-T2 no eran incluso fabricados.

Varias opciones también han sido especificadas para medios UTP: Categoría 3, 4, o 5E.
Las diferencias son el costo del cable y la capacidad de la tasa de transmisión, las cuales se incrementan con el número de categoría. Sin embargo, los requisitos de la tasa de transmisión corriente y el costo del cable no deberían ser factores de decisión al escoger cual categoría de cable instalar.

Para permitir futuras necesidades de transmisión de datos, cables menores a Categoría 5 no deberían ser considerados y como las tasas Gigabit son una necesidad, la Categoría 5E debió ser considerada:

- Los costos de instalación son esencialmente constantes para todos los tipos de cable UTP de par trenzado.

- Los costos por actualización de cableado (quitando el existente e instalando nuevo) son típicamente mayores que el costo de la instalación original.
- El cable UTP es compatible con el anterior UTP. Categorías mayores soportaran categorías menores de NICs, pero no viceversa.
- La vida física del cable UTP (décadas) es mucho más larga que la vida útil del equipo conectado.

### 1.8.2 Autonegociación — Un método alternativo para configurar automáticamente modos operacionales de links

El propósito de la autonegociación es encontrar una vía para que dos NICs compartan un link para comunicarse con algún otro, sin importar si ambos implementaron la misma versión de Ethernet o set de opciones.

La autonegociación es realizada totalmente dentro de las capas físicas durante el inicio del link, sin ninguna cabecera adicional o a la MAC o a capas mayores del protocolo.
La autonegociación permite que NICs basadas en UTP hagan el siguiente:

- Anunciar su versión de Ethernet y cualquier capacidad opcional al NIC en el otro extremo del link
- Reconocer de recibido y entender a los modos operacionales que ambos NICs comparten
- Rechazar cualquier modo operacional que no este compartido
- Configurar cada NIC para el modo operacional de más alto nivel que ambos NICs pueden soportar

La autonegociación esta especificada como una opción en 10BaseT, 100Base-TX y 100Base-T4, pero se requiere para las implementaciones 100Base-T2 y 1000Base-T.

La *Tabla 1-6* lista los niveles prioritarios de selección definidos (nivel más alto = mayor prioridad) para NICs Ethernet basadas en UTP.

| Nivel de selección | Modo operacional | Tasa máxima total de transferencia de datos (Mbps)[1] |
|---|---|---|
| 9 | 1000Base-T Full-duplex | 2000 |
| 8 | 1000Base-T Half-duplex | 1000 |
| 7 | 100Base-T2 Full-Duplex | 200 |
| 6 | 100Base-TX Full-duplex | 200 |
| 5 | 100Base-T2 Half-Duplex | 100 |
| 4 | 100Base-T4 Half-duplex | 100 |
| 3 | 100ase-TX Half-duplex | 100 |
| 2 | 10Base-T Full-duplex | 20 |
| 1 | 10Base-T Half-duplex | 10 |

[1] Debido a que la operación full-duplex permite dos vías de transmisión simultaneas, la tasa máxima total de transferencia para la operación full-duplex

***Tabla 1-6 Niveles de selección definidos de Autonegociación para NICs UTP***

La función de autonegociación en NICs basadas en UTP usa una integridad de secuencia de pulsos modificada 10Base-T en la cual los NLP's son reemplazados por ráfagas de pulsos de link rápidos (FLP's, Fast Link Pulses), como se muestra en la *Figura 1-28*.

Cada ráfaga FLP es una secuencia alternada reloj/datos (clock/data) en la cual los bits de datos en la ráfaga identifican los modos operacionales soportados por la NIC transmisora y también provee información usada por el mecanismo de handshake (saludo) de autonegociación. Si la NIC del otro lado del link es una NIC compatible pero no tiene capacidad de autonegociación, una función de detección paralela sigue permitiéndole ser reconocida. Una NIC que falla al responder a las ráfagas FLP y retorna solo NLP's es tratada como una NIC 10Base-T half-duplex.

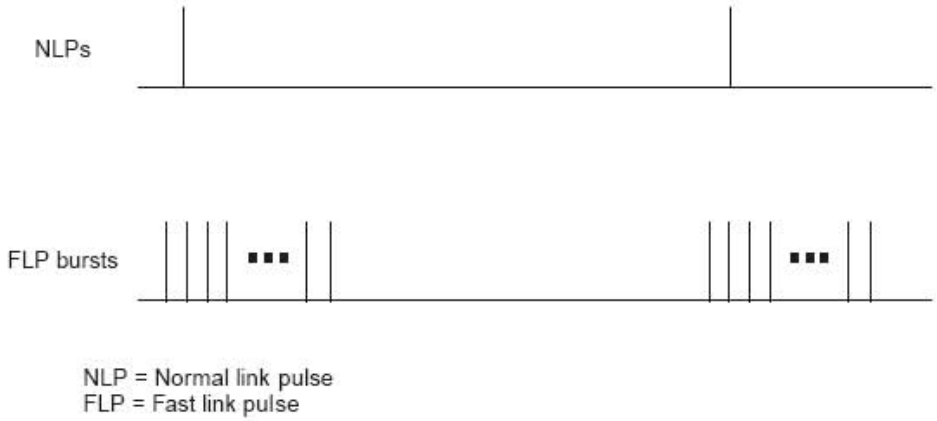



***Figura 1-28 Ráfagas FLP de autonegociación reemplazan NLP's durante el inicio del link***

De primera vista, puede parecer que el proceso de autonegociación siempre selecciona el modo soportado por el NIC con la capacidad menor, lo cual podría ser el caso si ambas NICs usan los mismos procedimientos de codificación y configuración del link.
Por ejemplo, si ambas NICs son 100Base-TX pero solo uno soporta la operación full-duplex, el modo operacional negociado será 100Base-TX. Desafortunadamente, las diferentes versiones 100Base no son compatibles con algún otra a 100 Mbps, y una NIC 100Base-TX full-duplex puede autonegociar con una NIC 100Base-T4 para operar en modo 10Base-T half-duplex.

La autonegociación en NICs 1000Base-X es similar a la autonegociación en sistemas basados en UTP, excepto que éste actualmente es aplicado solo a dispositivos compatibles con 1000Base-X, y es actualmente forzado a negociar solo operación half-duplex o full-duplex y dirección de flujo de control.

### 1.8.3 Los switches de red proporcionan una mejor alternativa para actualizaciones de red en CSMA/CD

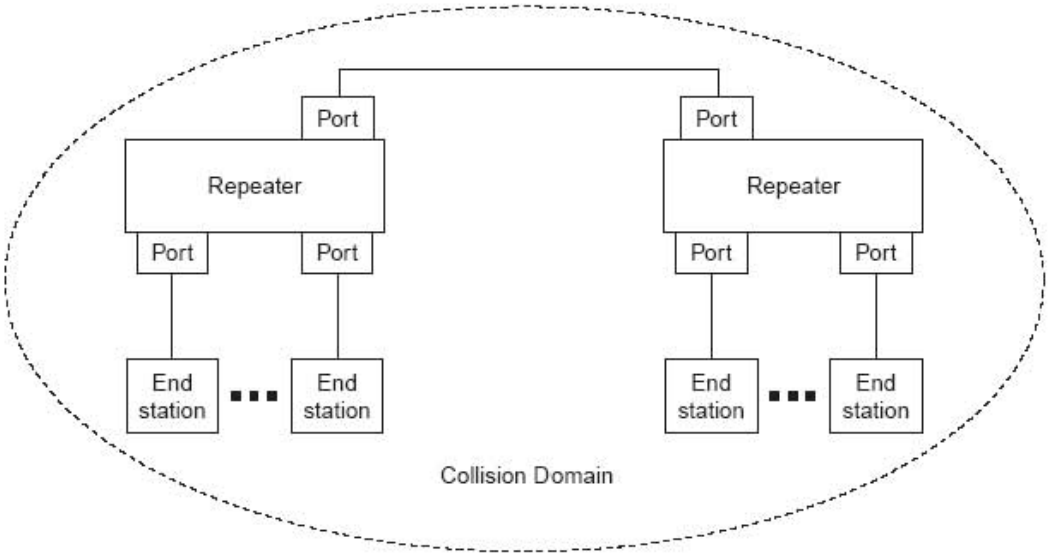
Los switches de red de precio competitivo llegaron a estar disponibles en el mercado poco después de mediados de los 90's y esencialmente hicieron los repetidores de red obsoletos para redes grandes. Aunque los repetidores pueden aceptar solamente una trama a la vez y entonces mandarla a todos los puertos activos (excepto al puerto en el cual esta siendo recibido), los switches son equipados con lo siguiente:

- Puertos basados en MAC con buffers de tramas de Entrada/Salida que aíslan efectivamente el puerto desde donde el trafico esta siendo enviado al mismo tiempo a o desde otros puertos en el switch
- Trayectorias de datos internas múltiples que permiten que a varias tramas ser transferidas entre diferentes puertos al mismo tiempo

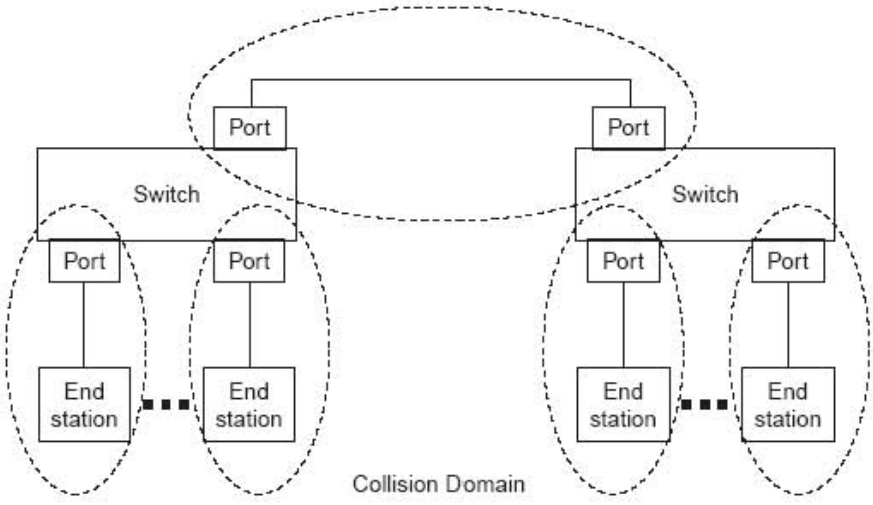
Éstos pueden parecerse aunque con diferencias pequeñas, pero producen un efecto mayor en la operación de red.

Debido a que cada puerto proporciona el acceso a un bridge de red de alta velocidad (High-Speed Network Bridge) que es el switch, el dominio de la colisión en la red es reducido a unas series de pequeños dominios en los cuales el número de participantes es reducido a dos –el puerto del switch y la NIC conectada- (ver *Figura 1-29*).

Además, ya que cada participante ahora está en un dominio privado de colisión, su disponibilidad de ancho de banda ha sido marcadamente aumentada, y esto fue hecho sin tener que cambiar la velocidad del link.




(a) Repeater-based CSMA/CD network




(b) Switch-based CSMA/CD network

***Figura 1-29 Reemplazar los repetidores de red (hubs) con switches reduce el dominio de la colisión a solo 2 NICs***

Considérese, por ejemplo, un grupo de trabajo de 48 estaciones con un par de servidores de archivo grandes y varias impresoras de red en una red a 100 Mbps CSMA/CD. El ancho de banda promedio, no contando vacíos intertramas y recuperación de colisión, seria 100/2= 2Mbps (servidores de impresión no generan trafico de red). Por otro lado, si el mismo grupo de trabajo siguiera siendo una red 10Base-T, en la cual los repetidores han sido reemplazados con switches de red, el ancho de banda disponible para cada usuario seria 10 Mbps.
Claramente, la configuración de red es tan importante como la velocidad cruda del link.

**Nota**
Para asegurarse que cada estación final sea capaz de comunicarse a tasa completa, los switches de red deberían ser No saturados (ser capaces de aceptar y transferir datos a tasa completa desde cada puerto simultáneamente).

### 1.8.4 NICs multivelocidad

La Autonegociación abrió la puerta al desarrollo de NICs multivelocidad de bajo costo que, por ejemplo soportan operación half-duplex y full-duplex bajo procedimientos de señalización 100Base-TX o 10Base-T. Las NICs multivelocidad permiten actualizaciones de red traseras en las cuales estaciones terminales 10Base-T pueden ser conectadas a puertos de switch 100Base-TX full-duplex sin requerir que la NIC en la PC sea cambiada.
Entonces, como más ancho de banda en necesario para PCs individuales, las NICs en esas PCs pueden ser actualizadas al modo 100Base-TX full-duplex.

### 1.8.5 Eligiendo componentes 1000Base-X y medios físicos

Aunque la *Tabla 1-7* demuestra que hay flexibilidad considerable de opciones en los medios de acoplamiento 1000Base-X, no hay flexibilidad total. Algunas opciones se prefieren sobre otras:

- NICs en ambos finales del link deben ser la misma versión 1000Base-X (CX, LX, o SX), y los conectores del link deben corresponder a los conectores del NIC.

- La especificación 1000Base-CX permite conectores de estilo 1 o estilo 2, pero el estilo 2 se prefiere porque algunos conectores de estilo 1 no son convenientes para operación a 1250 Mbps. Los links 1000Base-CX se piensan para el uso patch-cord dentro de comunicaciones cercanas y están limitadas a 25 metros.

- Las especificaciones 1000Base-LX y 1000Base-SX permiten o el factor pequeño SFF MT-RJ o los conectores duplex mas largos SC. Ya que los conectores SFF MT-RJ son solo la mitad del largo de los conectores SC duplex, y porque el espacio es un lujo, esto lleva a que los conectores SFF MT-RJ pueden llegar a ser los conectores predominantes.

- Los transceptores 1000Base-LX cuestan generalmente más que los transceptores 1000Base-SX.

- El rango de operación máximo para las fibras ópticas depende tanto de la longitud de onda de transmisión y del rango de ancho de banda modal (en MHz*Km) de la fibra. Ver *Tabla 1-7*.

Los rangos de operación mostrados en la *Tabla 1-7* son aquellos especificados en el estándar IEEE 802.3. En la práctica, sin embargo, el rango de operación máximo para los transceptores LX sobre fibra multimodo de 62.5 µm es aproximadamente 700 metros, y algunos transceptores LX han sido calificados para soportar un rango de operación de 10,000 metros sobre fibra monomodo (single mode).

| Diámetro del núcleo de la fibra / Ancho de banda modal | 1000Base-SX (Longitud de onda 850 nm) | 1000Base-LX (Longitud de onda 1300 nm) |
|---|---|---|
| Fibra multimodo 62.5 µm (200/500) MHz*km | 275 metros | 550 metros[1] |
| Fibra multimodo 50 µm (400/400) MHz*km | 500 metros | 550 metros[1] |
| Fibra multimodo 50 µm (500/500) MHz*km | 550 metros | 550 metros[1] |
| Fibra monomodo 10 µm | No soportada | 5000 metros |

[1] Los transceptores 1000Base-LX pueden también requerir el uso de un compensador, un patch-cord (cable) que acondiciona a los transceptores cuando se acoplan a algunas fibras multimodo existentes

***Tabla 1-7 Rangos máximos de operación para Fibras Ópticas Comunes***

### 1.8.6 Redes Ethernet de múltiples tasas

Dadas las oportunidades mostradas por el ejemplo en las secciones anteriores, no es sorpresa que las redes Ethernet más grandes son ahora implementadas con tasas de transmisión y medios de link mixtos, como se muestra en el modelo de cable mostrado en la *Figura 1-30*.

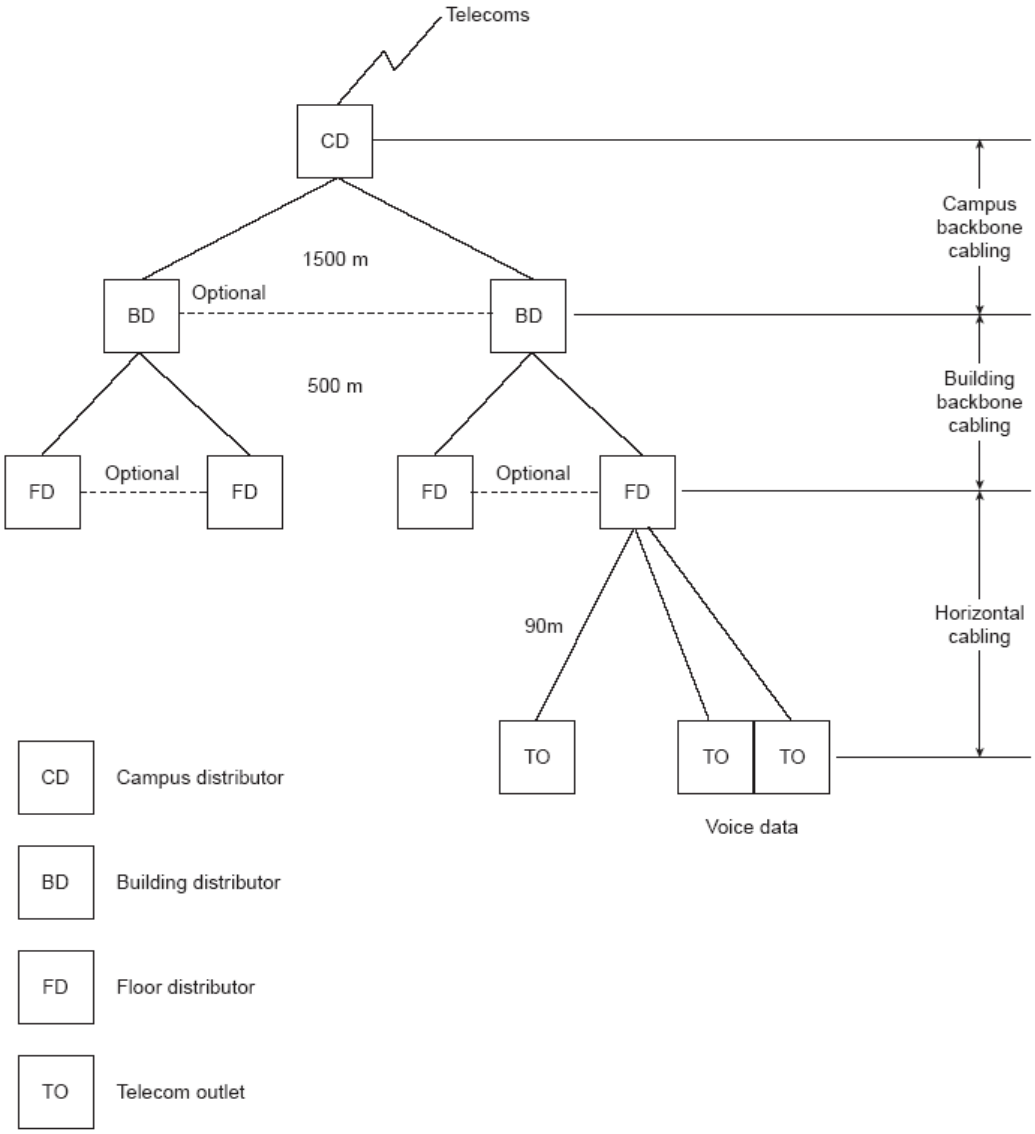



***Figura 1-30 Un ejemplo de topologías de red multitasa – el modelo de cable ISO/IEC 11801***

El modelo de cable ISO/IEC 11801 es el modelo de red en el cual se basa el estándar IEEE 802.3:

- **Distribuidor de campus** —El termino campus se refiere a una instalación con dos o más edificios en una área relativamente pequeña. Éste es el punto central del backbone del campus y el punto de conexión de telecomunicaciones con el mundo exterior.
  En LANs Ethernet, el distribuidor de campus sería típicamente un switch Gigabit con capacidad de interface de telecomunicaciones.

- **Distribuidor de edificio** —Este es el punto de conexión del edificio al backbone de campus. Un distribuidor de edificio Ethernet sería típicamente un switch a 1000/100 o 1000/100/10 Mbps.

- **Distribuidor de piso** —Este es el punto de conexión del piso al distribuidor del edificio. La ISO/IEC 11801 recomienda al menos un distribuidor de piso por cada 1000$m^2$ de espacio en ambientes de oficina, y si es posible, un distribuidor separado por cada piso en el edificio. Un distribuidor de piso Ethernet sería típicamente un switch de 1000/100/10 o 100/10 Mbps.

- **Toma de telecomunicaciones** —Este es el punto de conexión de red para las PC, estaciones de trabajo y servidores de impresión. Los servidores de archivo son típicamente colocados con y directamente al campus, edificio, o distribuidores de piso, tan apropiado como se intente usar.

- **Cableado de backbone de campo** —Este es típicamente cable sencillo o multimodo que interconecta el distribuidor de campo central con cada distribuidor de edificio.

- **Cableado de backbone de edificio** —Este es típicamente UTP Categoría 5 o mayor, o cable de fibra multimodo que interconecta el distribuidor de edificio con cada distribuidor de piso en el edificio.

- **Cableado horizontal** —Este es predominante UTP Categoría 5 o mayor, aunque algunas instalaciones se utiliza fibra multimodo.

Como en la selección del cable UTP, la opción del medio para links y nodos de red intermedios debería ser siempre hecho con mira en las tasas de transmisión futuras y la expectativa de vida de los elementos de la red. En los 90s, las tasas de transmisión en LANs se incrementaron 100 veces y para 2002 se incrementaron todavía otras 10 veces.

Esto no significa que todas —o aún algunas —estaciones finales y sus links de interconexión requerirán capacidad Gigabit. Significa, sin embargo, que más nodos de red centrales (tales como la mayoría de distribuidores de campus y muchos distribuidores de edificio) deberían ser equipados con capacidad Gigabit, y que todos los distribuidores de piso deben tener al menos capacidad de 100 Mbps. Esto también significa que todos los switches de red deberían estar no bloqueados y que todos los puertos deberían tener capacidad full-duplex, y que cualquier nuevo link de backbone de campus debería ser instalado con fibra de modo simple (single mode).

### 1.8.7 Adición de link — Estableciendo troncales de red de alta velocidad

La adición de link es una capacidad reciente y opcional de la MAC que permite varios links físicos para ser combinados en una troncal lógica de alta velocidad. Ésta provee los medios para incrementar la tasa efectiva de datos entre 2 nodos de red en múltiplos de la unidad de la tasa de transmisión individual del link más bien que en un paso de magnitud por orden.

La adición del link puede ser una vía efectiva en costo para proporcionar conexiones de alta velocidad en LANs Ethernet que están alcanzando la saturación con tasas de transmisión a 100 Mbps pero que no pero que no requerirá capacidad Gigabit, por lo menos a corto plazo.

Por ejemplo, la longitud máxima para links de fibra multimodo de 62.5µm es de 2000 metros a 100 Mbps, y la fibra multimodo ha sido siempre usada para links de campo tipo backbone.
La actualización lógica podría ser reutilizar estos links para una operación a 1000 Mbps, pero la longitud máxima soportable para fibra multimodo es de 700 metros y solo con 1000Base-LX. Si estos links existentes son mayores a 700 metros, agregando *n* links existentes soportara una tasa de transmisión efectiva de (100*n*) Mbps.

La adición de link debería ser vista como una opción de configuración de la red que es primariamente usada en las pequeñas interconexiones que requieren mayores tasas de datos que pueden ser provistos por links sencillos, como son los switch-to-switch y en servidor switch-to-file. Esta puede también ser usada para incrementar la confiabilidad de links críticos.
Links agregados pueden ser rápidamente reconfigurados (típicamente en cerca de 1 segundo o menos) en caso de falla del enlace, con bajo riesgo de tramas duplicadas o reordenadas.

La adición de links no afecta o al formato(s) de trama de datos de la IEEE 802.3 o a alguna de las capas superiores de la pila del protocolo. Es compatible con dispositivos anteriores con “agregation-unaware” que pueden ser usados con cualquier tasa de datos Ethernet (aunque esto no tiene sentido para 10 Mbps porque costaría probablemente menos procurar comprar un par de NICs de 100 Mbps).
La adición de links puede ser habilitada solo en links paralelos punto a punto y en aquellos que soporten operación full-duplex con la misma velocidad.

### 1.8.8 Administración de la red

Todas las especificaciones Ethernet de alta velocidad incluyen definiciones para manejo de objetos y agentes de control que son compatibles con SNMP (Simple Network Management Protocol) y que pueden ser usados para recopilar estadísticas acerca de la operación de los nodos de la red y para ayudar al manejo de la red. Debido a que la información del usuario es anecdótica en el mejor de los casos y viene generalmente primero el largo y después el hecho, todas las redes más grandes deberían ser configuradas por lo menos con switches manejados y servidores de red para asegurarse que problemas potenciales y cuellos de botella pueden ser identificados antes de que causen serios deterioros a la red.

### 1.8.9 Migrando a redes de alta velocidad

Ahora, debe ser aparente que la actualización de redes existentes típicamente no requiere equipamiento al por mayor o cambio de medios físicos, pero esto requiere conocimiento de la configuración de red actual y la ubicación de la red para problemas potenciales.
Esto significa que un sistema de manejo de red debe estar en un cierto lugar y que una base de datos del cable de la planta debería ser exacta y estar disponible. Esto es un consumidor de tiempo y siempre dificulta para determinar el tipo de link y la disponibilidad después de que los cables han sido jalados a través de la tubería, enterrados en la pared y puestos en bandejas para cable.

Los links son siempre el factor limitante en actualizaciones de red. Links existentes Categoría 5 deberían soportar todas las tasas Ethernet actuales desde 10 Mbps a 1000 Mbps, aunque estas deberían ser checadas para asegurarse de su capacidad para soportar tasas Gigabit. Si la red esta equipada con cable Categoría 3, algunos links tendrán que ser reemplazados antes de actualizar a 1000 Mbps. Una situación similar existe con fibra simple y multimodo.
La fibra multimodo no puede ser usada para todas las instalaciones backbone.
La fibra monomodo, por otro lado, no solo puede soportar todas las longitudes de backbone arriba de 10,000 metros a 1000 Mbps, sino también será capaz de soportar el uso de backbone en tasas de 10 Gigabits en el futuro.

El reemplazo del switch puede comenzar tan pronto como los links necesarios estén disponibles. Los switches existentes en el campus y en los niveles de distribución de edificio pueden ser siempre reutilizados en el edificio o en distribuidores de nivel de piso. Las NICs generalmente son reemplazadas para extender la vida útil de las estaciones finales. Etcétera.

## 1.9 10Gigabit Ethernet (XGbE o 10GbE)

10Gigabit Ethernet es una red Ethernet que opera a la velocidad mas rápida hasta ahora, el estándar para 10Gigabit Ethernet fue formalmente ratificado por el IEEE en Junio 12 del año 2002 y tiene por nombre suplemento IEEE 802.3ae.

El nuevo estándar 10Gigabit Ethernet contiene siete tipos de medios los cuales son diseñados para usarse en redes locales o mayores. Esto proporciona al sistema 10 Gigabit Ethernet la flexibilidad necesaria para operar en redes de área local (LAN), redes de área metropolitana (MAN), redes de área regional (RAN) y redes de área amplia (WAN).
Hay diferentes estándares para el nivel físico (PHY). La letra "X" significa codificación 8B/10B y se usa para interfaces de cobre. La variedad óptica más común se denomina LAN PHY, usada para conectar routers y switches entre sí. Aunque se denomine como LAN se puede usar con 10GBase-LR y -ER hasta 80km. LAN PHY usa una velocidad de línea de 10.3 Gbit/s y codificación 66B. WAN PHY (marcada con una "W") encapsula las tramas Ethernet para la transmisión sobre un canal SDH/SONET STS-192c.
La introducción del suplemento IEEE 802.3ae da una idea general de lo que será el estándar de 10 Gigabit Ethernet:

“Este suplemento para el estándar IEEE 802.3 da apoyo para extender la especificación del protocolo y la MAC 802.3 para una velocidad de operación a 10 Gb/s. Algunas subcapas de codificación físicas (Physical Coding Sublayers) conocidas como 10GBASE-X, 10GBASE-R y 10GBASE-W están especificadas, además de material de soporte adicional significativo para una Interfaz Independiente del Medio 10 Gigabit (XGMII, 10 Gigabit Media Independent Interface), una Unidad de Interfaz Agregada 10 Gigabit (XAUI, 10 Gigabit Attachment Unit Interface), una Interfaz de 16 bits 10 Gigabit (XSBI, 10 Gigabit Sixteen-Bit Interface) y gestión.

Las capas físicas especificadas incluyen 10GBASE-S, un transceptor serie de longitud de onda de 850 nm el cual usa dos fibras multimodo; 10GBASE-L4, un transceptor (WDM, Wavelength Division Multiplexing) de 1310 nm de longitud de onda el cual utiliza fibras monomodo o dos fibras multimodo; 10GBASE-L, un transceptor serie de 1310 nm el cual usa dos fibras monomodo, y 10GBASE-E, un transceptor serie de 1550 nm de longitud de onda el cual utiliza dos fibras monomodo.”

### 1.9.1 Nomenclatura 10Gigabit Ethernet

Los tipos de medio 10 Gigabit usan una serie de letras para indicar la longitud de onda que estos utilizan y el tipo de codificación utilizada.

Los tipos de codificación de señal 10 Gigabit Ethernet incluyen una “Subcapa de Interfaz WAN (WAN Interface Sublayer) llamada WIS” la cual permite al equipo 10 Gigabit Ethernet ser compatible con el formato de transmisión SONET (Synchronous Optical Network) STS-192c. El equipo SONET es comúnmente usado para llevar datos de comunicación a largas distancias, y el formato STS-192c provee una capacidad de carga de 9.58464 Gbps.
El subsistema WIS extiende el espacio entre tramas (interframe gap) lo necesario para obligar la capacidad efectiva de datos del sistema 10 Gigabit Ethernet a la capacidad de carga del STS 192-c.

En los tipos de medio 10GBASE-X, una “S” en la primera posición quiere decir que esta red opera con fibra óptica de una longitud de onda de 850 nanómetros (nm), una “L” opera con fibra de longitud de onda de 1310 nm y una “E” opera con 1550 nm. La letra “X” denota una codificación de señal 8B/10B, mientras la “R” denota codificación 66B y la ultima “W” denota la interfaz WIS que encapsula tramas Ethernet para transmisión sobre un canal SONET STS 192-c.

### 1.9.2 Tipos de medios 10 Gigabit Ethernet

Los tipos de medio **10GBASE-SR (“Short Range”)** y **10GBASE-SW** están diseñados para usarse sobre fibra multimodo (MMF, Multimode Fiber) de longitud de onda pequeña (850 nm). La meta del diseño de este tipo de medios va desde los 2 m a los 300 m de distancia, dependiendo del tipo y la calidad de la fibra multimodo. Mayores distancias son posibles dependiendo de la calidad del cable de fibra óptica usado.
El tipo de medio 10GBASE-SR esta diseñado para usarse sobre fibra negra, que es el aquel cable óptico que no esta en uso y que no esta conectado a ningún otro equipo. El tipo de medio 10GBASE-SW esta diseñado para conectarse a equipos SONET, el cual es típicamente usado para dar comunicaciones a larga distancia.

Los medios **10GBASE-LR** y **10GBASE-LW** están diseñados para usarse en fibra monomodo (SMF, Single Mode Fiber) de longitud de onda de 1310 nm. La meta del diseño de estos medios es para trabajar desde los 2 m hasta los 10 Km (32,808 feet), dependiendo del tipo de cable y la calidad de éste (distancias mayores son posibles). El medio 10GBASE-LR esta diseñado para usarse sobre fibra negra, mientras que el 10GBASE-LW esta diseñado para conectarse a equipo SONET.

Los medios **10GBASE-ER** y **10GBASE-EW** están diseñados para usarse sobre una fibra monomodo (SMF, Single Mode Fiber) de longitud de onda extra larga (1550 nm). La meta para el diseño de este medio es desde los 2 m hasta los 40 Km (131,233 feet), dependiendo del tipo y calidad del cable de fibra usado (distancias mayores son posibles). El medio 10GBASE-ER esta diseñado para usarse sobre fibra negra, mientras el 10GBASE-EW esta diseñado para conectarse a equipo SONET.

Finalmente está el medio 10GBASE-LX4, el cual usa tecnología de multiplexado y división de onda para enviar señales sobre 4 longitudes de onda de luz llevadas sobre un par simple o sobre cables de fibra óptica. El sistema 10GBASE-LX4 esta diseñado para operar a 1310 nm sobre fibra negra monomodo o multimodo. La meta del diseño de este medio va de los 2 m a los 300 m sobre fibra multimodo y de los 2 m a los 10 Km sobre fibra monomodo, con distancias mayores dependiendo del tipo y calidad del cable de fibra usado.

# CAPITULO 2

## Ethernet en la industria

## 2.1 Tecnología Ethernet

Basado en el modelo de referencia OSI (Open System Interconnection) para sistemas de comunicación, la tecnología Ethernet, los servicios y protocolos usados en Ethernet además de su clasificación dentro de la estructura de las capas en el modelo de referencia OSI se muestran a continuación.

### 2.1.1 Modelo de referencia OSI

El modelo de referencia OSI describe y estandariza la comunicación entre sistemas (dispositivos, computadoras) en una arquitectura de red abierta. Funciones, necesarias para la comunicación son subdividas en siete capas de función. Para esta abstracción, este complejo proceso de comunicación esta simplificado y subdividido en pequeñas unidades lógicas. Una ventaja importante de la realización de la comunicación en capas sencillas es también la posibilidad de intercambiar la implementación técnica de una capa independiente desde otras capas. Por ejemplo, es posible intercambiar el medio de transmisión sin ningún problema. La funcionalidad continúa sin ningún cambio en las otras capas.

De la Capa 1 a la 4 también llamadas capas inferiores están orientadas a red. Las capas de la 5 a la 7 están orientadas a aplicación y son llamadas capas superiores. Cada capa inferior respectiva provee sus servicios a la capa de arriba bien definidas por medio de interfaces.

**La Capa 1, la Capa Física** representa una transferencia insegura a través del medio físico, donde los datos son transmitidos bit por bit. La especificación incluye también distribución de pines, voltajes y cable.
**La Capa 2, la Capa de Enlace de Datos** describe una detección de errores en la transmisión de los bits empaquetados en bloques entre dos dispositivos conectados directamente. También, el acceso correcto al medio de transmisión es manejado aquí.
**La Capa 3** provee las trayectorias entre transmisor y receptor a través de una o varias redes y es llamada **Capa de Red**.
**La Capa 4, la Capa de Transporte** es la responsable de la transmisión libre de errores y una secuencia de transmisión compatible de los datos entre los dispositivos terminales y es una abstracción de las tecnologías de red y topologías subyacentes.
**La Capa 5, la Capa de Sesión** establece y termina conexiones entre dispositivos y los observa. De este modo esta capa no es necesaria para la comunicación no conectada.
**En la Capa 6**, los datos de la **Capa de Presentación** a ser transmitidos son convertidos en un formato común (sintaxis de transferencia) y cambiados al lado receptor en la sintaxis necesaria ahí.
**La Capa 7** proporciona servicios para los participantes en la red, por ejemplo la transmisión de archivos o el acceso a una computadora central. Estos servicios o protocolos son siempre interfaces a servicios generales y representan la **Capa de Aplicación**.

Antes de que los datos de usuario (proceso de aplicación) puedan ser enviados sobre el medio Ethernet, estos tienen que ser pasados a través de la pila del protocolo desde las capas superiores a las inferiores eventualmente para ser insertadas en tramas de la capa inferior particular (encapsulación). Después de que un paquete de datos es enviado sobre la capa mas baja (medio físico), los datos contienen pases hacia arriba a través de todas las capas superiores hasta el dispositivo receptor hasta que consigue la capa de aplicación y de nuevo, el proceso de aplicación.

Todo el proceso requiere una interacción lógica dentro de cada capa para completar la conexión de red, como se muestra en la siguiente figura:

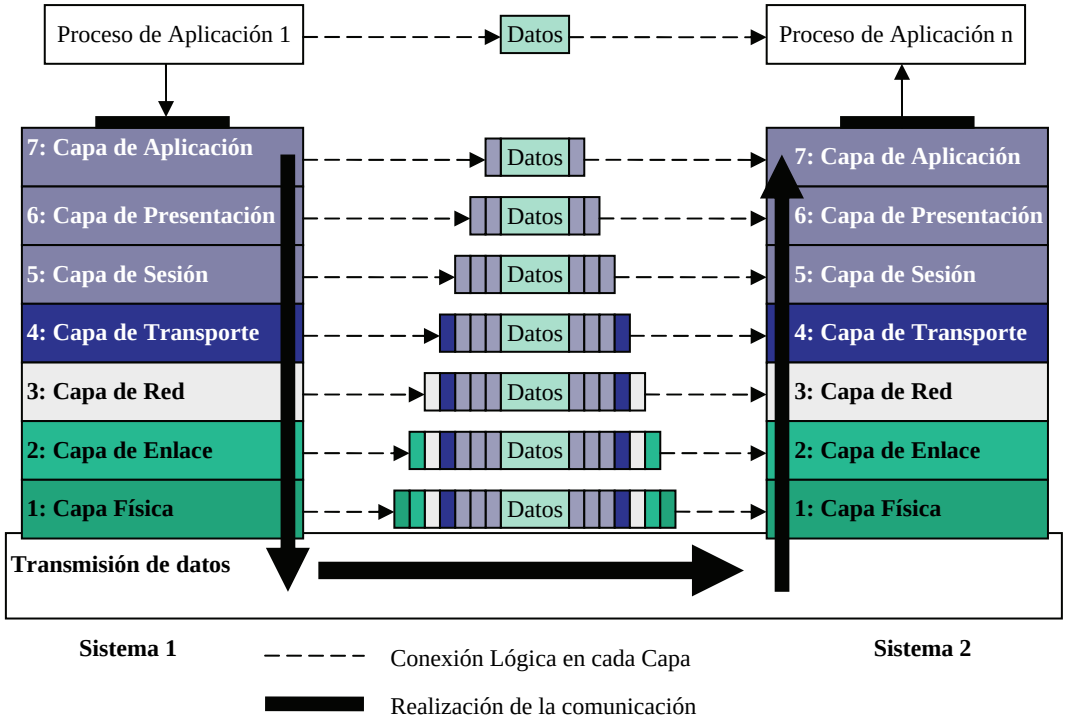



*Figura 2-1: Intercambio de datos en el Modelo de referencia OSI*

### 2.1.2 Suite del protocolo Ethernet

Una comunicación estandarizada es el requerimiento básico para la interoperabilidad entre sistemas, y Ethernet representa tal estándar. Ethernet por si mismo realiza las Capas 1 y 2 del modelo de referencia OSI y es especificado dentro del estándar IEEE 802.1-3. Las capas superiores implementan los protocolos de transporte Internet IP (Capa 3) y TCP/UDP (Capa 4).
Ethernet junto con las especificaciones TCP/UDP e IP es también llamado Suite del Protocolo Internet (Internet Protocol Suite), considerando que TCP/IP es siempre usado como un sinónimo para la suite entera del protocolo. De las Capas 5 a 7 proveen protocolos de aplicación como son FTP, Telnet, SMTP, NSP, SNMP así como varios protocolos industriales Ethernet como es Modbus/TCP.

Los protocolos de la suite del protocolo Ethernet son encapsulados dentro de otro. Esto significa que el protocolo entero de una capa es situado dentro del campo de datos del protocolo en la capa de abajo.

#### *Capa 1: Capa física*

Ethernet es un bus lógico. Todos los paquetes de datos serán recibidos por todos los participantes. Pero serán procesados solo aquellos donde la dirección de destino sea igual a su propia dirección o aquellos que son direccionados a todos o a varios al mismo tiempo (broad o multicasting). Con respecto al estándar IEEE 802.3, la trama Ethernet transmitida bit por bit tiene el formato descrito en la siguiente figura:

| Preámbulo | Destino | Fuente | Campo de tipo | Campo de datos | Chequeo |
|---|---|---|---|---|---|
| 8 Byte | 6 Byte | 6 Byte | 2 Byte | 46 – 1,500 Byte | 2 Byte |

*Figura 2-2 Marco Ethernet estándar*

Cada paquete de datos será transmitido bit por bit en el medio físico. El flujo de bits se empieza con preámbulo especial usado para sincronizar al transmisor con todos los receptores. El preámbulo es sucedido por la dirección destino, la dirección fuente y el campo de datos. Este campo de datos es usado para distinguir entre protocolos de capas superiores. Siguiendo a esta cabecera los datos de usuario son transmitidos y el flujo de bits es finalizado con el campo de comprobación (Checksum field) y un vacío de "silencio" entre mensajes en el medio físico.

En el controlador Ethernet del receptor los datos transmitidos serán checados de errores por el campo checksum. Si no hay errores detectados los datos serán pasados a la siguiente capa superior.
En caso de que un error sea detectado el respectivo paquete será rechazado y el emisor no sabrá esto.

Las direcciones del transmisor y el receptor, integradas al flujo de bits del mensaje son dadas por la llamada dirección MAC la cual es especificada en la Capa 2.

| | |
|---|---|
| Preámbulo | Usado para sincronización del receptor e indica el inicio de la trama Ethernet |
| Destino | Dirección de recepción (MAC ID) |
| Fuente | Dirección destino (MAC ID) |
| Campo de tipo | Tipo del protocolo superior de la pila (por ejemplo TCP/IP) |
| Campo de datos | Contiene los datos transferidos desde la estación fuente a la estación destino |
| Chequeo | Contiene un valor de Chequeo de Redundancia Cíclica (CRC) usado para chequeo de errores |

***Tabla 2-1 Contenido de una trama Ethernet estándar***

### *Capa 2: Capa de enlace de datos*

Debido a que cualquier dispositivo Ethernet podría ser instalado en la misma red con otros dispositivos también de diferentes fabricantes, la dirección MAC (también llamada MAC ID) tiene que ser única en el mundo. Un valor de 48 bits es usado para eso, usualmente dado en lenguaje hexadecimal, por ejemplo: 00-C0-3D-AA-09-23. Éste se divide en un numero de identificación del fabricante (los primeros tres bytes) y un numero de serie consecutivo del adaptador (los tres bytes restantes).

También, dentro de esta capa el acceso al medio de transmisión físico (Medium Access Control, MAC) es especificado con el mecanismo de acceso CSMA/CD (Carrier Sense Multiple Access / Collision Detection).
Básicamente, cada dispositivo conectado a la red puede usar la red para transmisión de datos en cualquier momento – a condición de que la red no este en uso. Lo segundo es checar antes de enviar (CS, Carrier Sense). Pero también es posible que varias estaciones detecten un red libre al mismo tiempo y empiecen a enviar datos (MA, Multiple Access) o causado por tiempos de inicio de la señales, la transmisión de una estación será detectada por otra queriendo enviar después de comenzar su propia transmisión (CD; Collision Detect). Todas las estaciones emisoras entonces pararan su transmisión y empezaran un nuevo intento después de un tiempo dado con un factor aleatorio. Este acto puede repetirse mientras el valor del periodo de espera generado se incremente con cada colisión sucedida directamente. Así lo que ocurre es que un dispositivo que ha estado esperando tiene menor probabilidad de acceder al medio de transmisión que dispositivos que han intentado después de comenzar una transmisión.

### *Capa 3: Capa de red*

La Capa 3 implementa el Protocolo Internet (IP) para administrar el ruteo de datagramas de una red a otra. Actualmente se utiliza IP versión 4 (IPv4) con un rango de direcciones de 32 bits. Estos 4 bytes marcan la red (Net ID) así como el dispositivo terminal (Host ID).

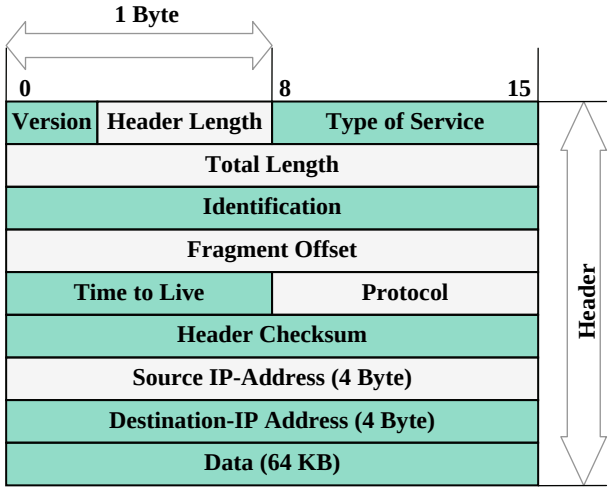



***Figura 2-3 Estructura del Protocolo IPv4***

Como una dirección IP en una red a nivel mundial como es Internet tiene que ser única, la reservación y asignación de direcciones son controladas por el IANA (Internet Assigned Numbers Authority).
Las direcciones son subdivididas en 3 clases: Clase A (para redes grandes), Clase B (para organizaciones como son las universidades) y Clase C (misceláneas). Además, existen las redes de Clase D y E usadas para la investigación y para propósitos especiales.

Basada en una descripción de direcciones IP de 4 bytes, una red Clase A tiene un arreglo del primer byte de dirección para la Net ID y 3 bytes para el Host ID; una red de Clase B tiene un arreglo de los dos primeros bytes de dirección para la Net ID y dos para el Host ID y la red Clase C tiene un arreglo de los tres primeros bytes de dirección para la Net ID y uno para el Host ID.

Algunos espacios de dirección así como direcciones son reservados para propósitos especiales. Por ejemplo la dirección mas alta en una red esta reservada como dirección destino indicando mensajes broadcast. Por ejemplo, en la red Clase C con la Net ID 131.32.140 la dirección IP 131.32.140.255 es usada para broadcast. Para mensajes multicast el espacio de direcciones desde 224.0.0.0 hasta 239.255.255.255 están reservadas. Ver subcapítulo 2.4.2 - Topologías lógicas.

Con la tabla ARP (Address Resolution Protocol) el software IP resuelve la dirección Ethernet de un dispositivo de la dirección IP. Cada dispositivo maneja su propia tabla dinámica ARP. Si no hay todavía una entrada para una dirección dedicada, un mensaje broadcast es enviado a la red (petición ARP). Este mensaje es direccionado a la dirección Ethernet FF-FF-FF-FF-FF-FF.
Mensajes a esta dirección serán leídos por todas las estaciones. El dispositivo apropiado reconoce su propia dirección IP y envía un mensaje de respuesta ARP el cual contiene la dirección Ethernet buscada. Ahora el dispositivo que pregunto puede completar la tabla ARP y dar los datos junto con la dirección Ethernet del dispositivo de destino al protocolo Ethernet.

El ICMP (Internet Control Message Protocol) da funcionalidades de control de red y es usado para transmitir información de estado, control y error entre nodos sencillos de una red. Para ese propósito un formato de paquete propio es usado, el cual es insertado en la parte de datos de un paquete IP. Los mensajes ICMP hacen posible analizar fuentes de error, aunque la transmisión IP por naturaleza es sin conexión y por lo tanto no da garantía de una transmisión exitosa. Un conocido ejemplo para la funcionalidad ICMP es el PING (Packet Internet Ghoper) el cual se realiza usando los paquetes ICMP Echo Request e ICMP Echo Reply.
IGMP (Internet Group Management Control) provee un servicio de intercambio de mensajes usado por los nodos de red para intercambiar información de administración para grupos receptores multicast. Esto posibilita a todos los dispositivos de una red física a saber a que grupo multicast pertenece un dispositivo especial.

Por lo tanto, interrogantes especiales IGMP (IGMP query) y mensajes de reporte son intercambiados por los nodos de red posibilitando a todos los nodos con funcionalidad de ruteo para detectar y observar los nodos pertenecientes a un grupo multicast. Usando el IGMP snooping (fisgoneo IGMP) los nodos de red pueden tratar con la información contenida en mensajes IGMP para manejar sus propias listas de ruteo de mensajes multicast por medio de una sencilla escucha pasiva de interrogantes IGMP y mensajes de reporte. Esta tecnología es siempre usada dentro de switches industriales y dispositivos de ruteo.

IPv6 es el nuevo protocolo Internet en versión 6 (1998) y reemplaza el llamado IPv4. Lo perceptible en IPv6 es el incremento del rango de direcciones a 128 bits. Comparando esto significa que en cada milímetro cuadrado de la superficie de la tierra es posible direccionar más de $665x10^{15}$ objetos.
Por esta razón el posible número de direcciones será suficiente en contraste a IPv4, por lo tanto la cabecera del datagrama fue modificada. Está fue simplificada y diseñada para modularidad y flexibilidad en el uso de cabeceras de extensión opcionales. La posibilidad de asignación prioritaria fue introducida también. Una nueva etiqueta de flujo habilita el mapeo de paquetes en flujos de datos para incrementar la eficiencia del procesamiento de paquetes. De este modo los routers pueden procesar paquetes más rápido con una conexión, sin analizar la cabecera completa. Una considerable reducción del esfuerzo del router también resulta en el hecho de que ya no se tiene cuidado de la fragmentación de paquetes.
Similar a las extensiones IPSec de IPv4 nuevos mecanismos de seguridad fueron introducidos en IPv6. En esencia esto significa que el contenido de un paquete puede ser encriptado contra la lectura y que una autenticación del receptor, transmisor y contenido del paquete es posible en la Capa 3 OSI.

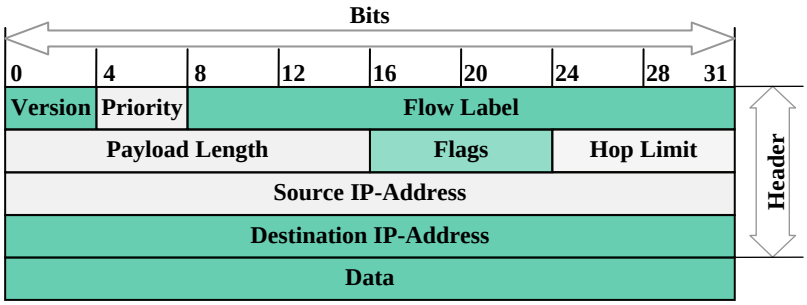



***Figura 2-4 Estructura del Protocolo IPv6***

La clasificación de redes fue también cambiada. Al lado de una diferenciación de rangos validos en direcciones globales (correspondientes a direcciones publicas en IPv4), las direcciones de sitios locales (IPv4, privadas), las direcciones de enlaces locales y direcciones de nodos locales, dentro de IPv6 los siguientes tipos de direcciones son definidas: Multicast, Anycast y Unicast.
Las direcciones Unicast identifican una interfaz sencilla. Ellas son diseñadas para un algoritmo de ruteo en el que sus decisiones están basadas en la correspondencia mas larga posible de una dirección dada. La estructura de la dirección es solo importante para la asignación, pero no para el ruteo. Las direcciones Anycast son un subconjunto especial de direcciones Unicast. Son usadas para enviar datos a múltiples interfaces, pero solo la interfaz que esta localizada mas cerca del emisor recibirá el paquete. Las direcciones Multicast pueden también representar más de una interfaz, pero en este caso todas las interfaces recibirían todos los datos. Las direcciones Broadcast provistas por IPv4 no están ya disponibles, por lo tanto todos los protocolos que utilizan Broadcast ahora son implementados vía Multicast.

El NDP (Neighbour Discovery Protocol) es nuevamente introducido con IPv6 y reemplaza varios protocolos de IPv4 (ARP, ICMP Router Discovery, ICMP Redirect).

El NDP realiza entre otras cosas las siguientes funciones:

- Búsqueda de routers dentro de la red local (Router Discovery)
- Distinción automática entre destinos en el mismo enlace y destinos los cuales pueden ser alcanzados solo vía router (Prefix Discovery)
- Detección de direcciones Capa 2 (MAC) de computadoras en el mismo enlace (Address Resolution)
- Monitoreo de si computadoras próximas son alcanzables (Neighbour Unreachability Detection)
- Si se detecta que un router no se puede alcanzar un router será automáticamente buscado
- Prueba de si una dirección ya esta en uso (Duplicate Address Detection)
- Asignación automática de dirección (Address auto configuration)

En principio, IPv6 provee la posibilidad de una configuración de falta de estado o (ya en IPv4) la autoconfiguración vía DHCP.

### *Capa 4: Capa de transporte*

Dentro de esta capa los protocolos TCP y UDP son implementados. El protocolo TCP (Transmission Control Protocol) es un protocolo basado en conexión diseñado para un transporte de datos libres de errores del tipo ping-pong con grandes tamaños de paquete.

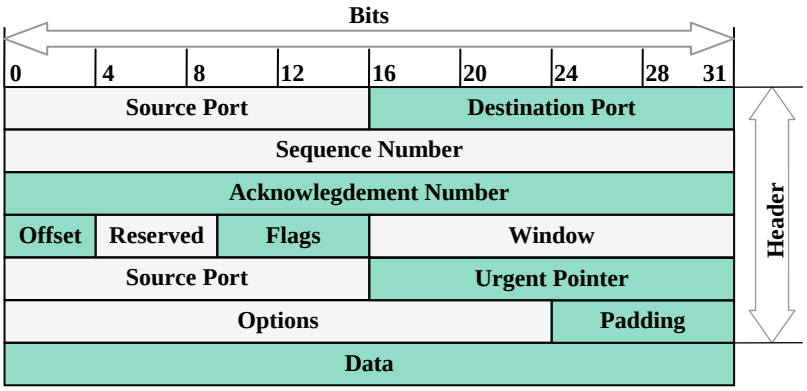



*Figura 2-5 Pila del Protocolo TCP*

La recepción libre de errores de un paquete es verificada por el dispositivo transmisor con conocimientos de disparo por parte del receptor. Si el arribo de un paquete no es conocido dentro de cierto tiempo el emisor reenvía el respectivo paquete de nuevo. De este modo, no solo una detección de error sino también la reparación del mismo pueden ser realizadas. Un dispositivo puede establecer varias conexiones a otras estaciones al mismo tiempo. También la conexión de la transmisión por si misma es checada por TCP.

Una conexión TCP es establecida y usada en la siguiente forma:

1. Como primer paso el dispositivo iniciando la conexión TCP (algunas veces llamado cliente) envía un mensaje SYN a la pareja de comunicación deseada (algunas veces llamado servidor) indicando la intención de establecer una conexión TCP y nombrando el numero de puerto del servidor, el cliente será conectado al numero de secuencia inicial (Initial Sequence Number, INS) de la comunicación.
2. El servidor responderá a este primer mensaje con un mensaje SYN propio conteniendo su propio ISN.
3. Adicionalmente el servidor enviara un mensaje de conocimiento conteniendo el ISN del cliente incrementado en uno.
4. El cliente entonces conocerá en el mensaje SYN del servidor su propio mensaje conteniendo el ISN del servidor incrementado en uno.

Después de este proceso de handshake (saludo) de tres vías, ambos, cliente y servidor intercambiaran mensajes en una forma controlada con mensaje y conocimiento de cada mensaje para verificar la estabilidad de la conexión TCP abierta. La terminación de la conexión es también hecha por un handshake de tres vías enviando y reconociendo la finalización de los mensajes (FIN).

Si la conexión se rompe, TCP informa directamente a la capa superior. En la suite del protocolo Internet ésta es la aplicación de software correspondiente.

Los puertos integrados en los mensajes sirven como interfaces a las aplicaciones. Puertos especiales para varias aplicaciones (por ejemplo el puerto 23 para Telnet) están reservados, si no entonces los puertos a ser usados son coordinados durante el establecimiento de la conexión. La combinación de una dirección IP de un dispositivo y el número de puerto de una aplicación corriendo en este dispositivo es llamada un Socket. Por lo tanto, un Socket representa un punto terminal de comunicación único en el mundo.

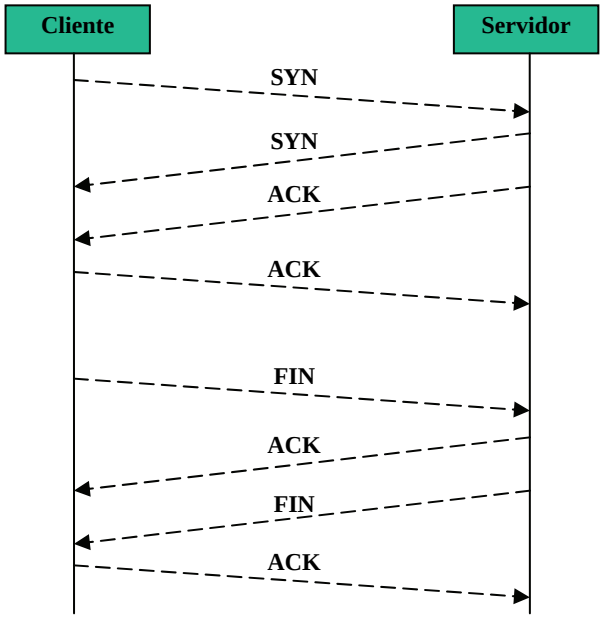



***Figura 2-6 Establecimiento de Conexión y Terminación TCP***

También UDP (User Datagram Protocol) realiza la Capa 4 correspondiente al modelo de referencia OSI, pero en comparación con TCP, UDP es un protocolo de una vía. Esto significa que el emisor no recibe ninguna respuesta acerca de la transmisión de datos correcta o perdida.

La transmisión vía UDP es mas rápida y el tamaño del protocolo es menor que TCP, pero los errores no son reparados. Un control de errores debe ser provisto por la aplicación la cual es direccionada vía puertos como en TCP. UDP es usado si es más importante recibir los datos actuales de un proceso por ejemplo, que cada paquete de forma completa. Por lo tanto, UDP es especialmente adecuado para transferencia de datos cíclicos de forma rápida.

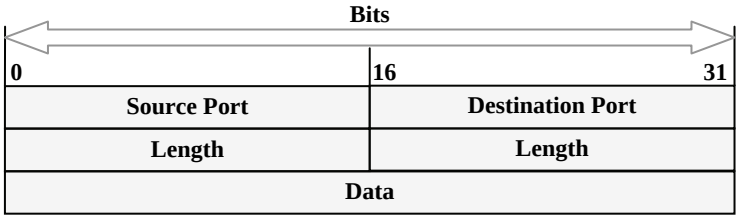



*Figura 2-7 Pila del Protocolo UDP*

### *Capa 7: Capa de aplicación*

El uso simple de un medio de transferencia común no significa automáticamente que todos los dispositivos conectados son capaces de comunicarse con algún otro. Siempre, esto es comparado con la telefonía: es posible telefonear a todo el mundo, el establecer una conexión no es el problema, el problema es entender lo que cada pareja de comunicación tiene que habar en un lenguaje común.
Aplicado esto al modelo de referencia OSI, significa que una comunicación abierta y uniforme hasta la capa de aplicación es necesaria.

En el mundo de la oficina un amplio rango de protocolos de aplicación, conocidos como estándares TI están disponibles, por ejemplo FTP, HTTP, etc. Por otro lado, en el lado de la comunicación industrial la tecnología Ethernet esta penetrando más y más, diferentes protocolos y especificaciones incompatibles con cada uno están en uso.

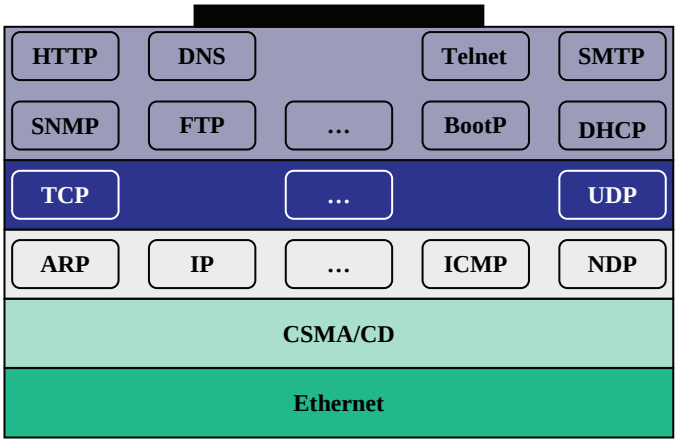



*Figura 2-8 Protocolos dentro del Modelo de Referencia OSI*

Soluciones basadas en Ethernet van a ser provistas por ejemplo la ODVA con EtherNet/IP, el Grupo Modbus-IDA con Modbus/TCP & RTPS, y el PNO (Profibus Nutzer/User Organisation) con PROFINET.

### 2.1.3 Posición de los protocolos dentro del modelo de referencia OSI

Los diferentes protocolos nombrados dentro de este subcapítulo son integrados dentro de las diferentes capas del modelo de referencia OSI. La tabla siguiente presenta una visión general de varios protocolos importantes que se usan dentro de la tecnología Ethernet y siempre se hace referencia de estos en todas las publicaciones.

| | | | |
|---|---|---|---|
| IP | Protocolo Internet (Internet Protocol) | IP es un protocolo que da un datagrama de no conexión poco fiable dando servicios basados en una estricta estructura de datagrama. | Capa 3 |
| APR | Protocolo de Resolución de Direcciones (Address Resolution Protocol) | ARP da un mapeo dinámico desde direcciones IP a direcciones de hardware (MAC) basado en un set de peticiones predefinidas y mensajes de respuesta | Capa 3 |
| ICMP | Protocolo de Control de Mensajes Internet (Internet Control Message Protocol) | ICMP da la posibilidad para comunicar mensajes de error así como el status de información de los nodos de red. | Capa 3 |
| IGMP | Protocolo de Manejo del Grupo Internet (Internet Group Management Protocol) | IGMP es usado para manejar sets de dispositivos pertenecientes a grupos multicast. Basado en dispositivos IGMP se pueden unir o separar grupos multicast y puede enviar reportes de status. | Capa 3 |
| NDP | Protocolo Descubridor de Vecino (Neighbour Discovery Protocol) | NDP provee la posibilidad de manejar propiedades de red y relaciones basadas en IPv6. Este reemplaza algunos protocolos usados en IPv4 como es ARP. | Capa 3 |
| TCP | Protocolo de Control de Transmisión (Transmission Control Protocol) | TCP da un mensaje orientado a conexión entregando servicios basados en conexiones estables y observables. | Capa 4 |
| UDP | Protocolo de Usuario de Datagramas (User Datagram Protocol) | UDP da un servicio simple, orientado a datagramas y con mensajes sin conexión. | Capa 4 |
| BootP | Protocolo Bootstrap (Bootstrap Protocol) | Provee una configuración IP asignada y estática para una dirección MAC dada, MAC address. | Capa 5-7 |
| DHCP | Protocolo de Configuración de Huésped Dinámico (Dynamic Host Configuration Protocol) | Método para asignación dinámica de una configuración IP (dirección IP, mascara de subred) durante el proceso de inicio de un dispositivo o para un intervalo de tiempo especifico. | Capa 5-7 |
| DNS | Servidor de Nombre de Dominio (Domain Name Server) | Resolución de Nombres en la Internet y redes LAN. Nombres de PC's y websites serán transferidos a la dirección IP apropiada por medio de DNS. | Capa 5-7 |
| SMTP | Protocolo de Transferencia de Mail Simple (Single Mail Transfer Protocol) | Protocolo Internet el cual proporciona servicios de E-mail. | Capa 5-7 |
| SNMP | Protocolo de Manejo Sencillo de Red (Simple Network Management Protocol) | Método para obtener información de status de componentes de red y PC's. | Capa 5-7 |
| Telnet | Terminal sobre Red (Terminal Over Network) | Telnet es una terminal de acceso remoto virtual y proporciona una función de comunicación orientada de 8 Bytes bidireccionales en PC's remotas. | Capa 5-7 |
| HTTP | Protocolo de Transferencia de Hipertexto (Hypertext Transfer Protocol) | HTTP es un protocolo basado en cliente-servidor usado para transportar información en la World Wide Web. El propósito original era dar una vía para publicar y recibir paginas HTML. | Capa 5-7 |
| FTP | Protocolo de Transferencia de Archivos (File Transfer Protocol) | FTP es un protocolo basado en cliente-servidor para transferir archivos de datos entre cliente y servidor en ambas direcciones. | Capa 5-7 |

***Tabla 2-2 Ejemplos de Aplicación de los Protocolos***

## 2.2 Diferencias entre la oficina y la planta industrial

Durante los 90's del siglo pasado, la PC y la tecnología Ethernet (además de la suite de protocolos TCP/IP) entraron al área de oficina. Compañías lideres de las tecnologías de información como Microsoft, Apple, Epson, Siemens y otras han usado el nuevo estándar establecido como IEEE 802.3 para desarrollar una única y distribuible ruta de comunicaciones independiente entre sistemas PC y sus dispositivos periféricos como son por ejemplo, impresoras, scanners, cámaras digitales o faxes.
A pesar de nuevas tecnologías emergidas como USB y Bluetooth, las comunicaciones basadas en Ethernet y TCP/IP han sido establecidas como estándares forzosos dentro de los sistemas de comunicaciones en oficinas. Dentro del área comercial como del consumidor privado todas las comunicaciones basadas en Ethernet son aceptadas.

Hoy en día, comunicaciones basadas en Ethernet están incrementándose de manera importante en las fábricas. Fabricantes, vendedores y usuarios finales de dispositivos de automatización están apuntando a los beneficios técnicos, económicos y de aplicación que los sistemas de comunicación basados en Ethernet dan en tasa mas alta comparada a sistemas de fieldbus convencionales o el costo reducido de las tarjetas de red resultando de la escala de efectos económicos.

Pero las aplicaciones simples de oficina basadas en comunicación Ethernet en las fábricas son imposibles. Aquí, los sistemas de comunicación basados en Ethernet son más que solo conectar algunos enchufes dentro del tomacorriente de pared y poner en los aparatos. La razón principal para esa circunstancia son los diferentes requerimientos en los dispositivos y en los componentes activos y pasivos dentro de una oficina y un sistema de comunicación de una fábrica.

Las principales diferencias son:

- La cantidad, las condiciones temporales de existencia y la complejidad de datos los cuales tienen que ser cambiados usando el sistema de comunicación.
- Las propiedades temporales del sistema de comunicación tienen que garantizarse con respecto al determinismo y a la velocidad de la comunicación.
- La estabilidad, seguridad; y la seguridad del sistema de comunicación tiene que garantizarse y finalmente
- La necesaria resistencia de los sistemas de comunicación contra influencias ambientales, térmicas o impactos electromagnéticos.

Dentro de todas las áreas mencionadas los sistemas de comunicación industrial tienen que cumplir requerimientos más altos que los sistemas de comunicación en oficinas. Además de estos requerimientos los nuevos sistemas de comunicación basados en Ethernet tienen que ser más amigables dentro de áreas de diseño, implementación, aplicación y mantenimiento.
Esto es representado en la figura siguiente.

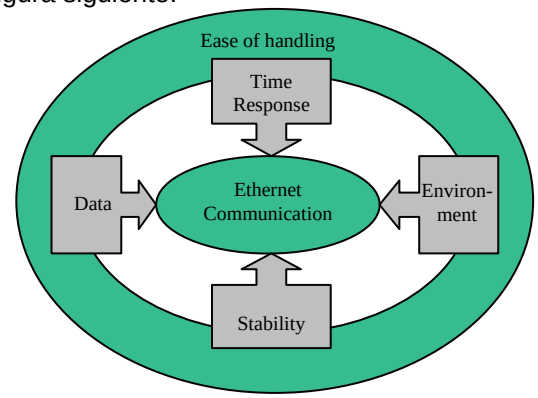



***Figura 2-9 Requerimientos adicionales para un sistema de comunicación industrial basado en Ethernet***

A continuación se analizaran con más detalle los 5 aspectos antes citados en la figura.

Dentro del área de oficina los sistemas de comunicación usualmente conectaran PC's individuales con otras, PC's con sistemas servidores, PC's con sistemas de impresión, PC's con scanners de red, PC's con algún otros aparatos periféricos de red y PC's con la Internet. Un ejemplo de un sistema de comunicación de oficina es presentado en la siguiente:

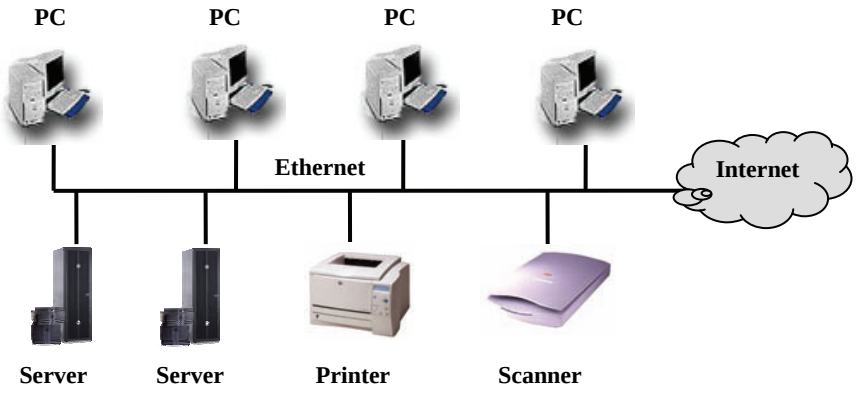



***Figura 2-10 Ejemplo de una red de oficina típica***

La comunicación basada en la interacción de dos compañeros de comunicación dentro de una red de oficina esta basada principalmente en el paradigma cliente-servidor. El que inicia la interacción actúa como cliente pidiendo un servicio especial dentro del servidor para recibir un dato especial (por ejemplo en el caso de actividad de descarga desde un servidor de datos), para comenzar una actividad especial dentro del servidor basada en transmisión de datos (por ejemplo para imprimir un documento), o para generar un estado especial dentro del servidor (por ejemplo para guardar datos dentro de una base de datos por medio del acceso a una base de datos).

Los datos afectados serán principalmente transmitidos usando los protocolos usuales de Internet como FTP, HTTP, SNMP, DHCP, y otros y alternativamente, usando una conexión a un socket dedicado entre dos aplicaciones corriendo del lado del cliente y del servidor sabiendo en el avance el contenido de los datos transmitidos. El tamaño de los datos transmitidos usualmente esta en el rango de un par de kilobytes a algunos cientos de megabytes.

En la industria los aparatos integrados en un sistema de comunicación son diferentes. Adicionales a los dispositivos basados en PC los cuales pueden ser usualmente encontrados dentro de una red de oficina también están aparatos especiales como Controladores Lógico Programables (PLC's), sistemas de control CNC, sensores como por ejemplo codificadores rotatorios y codificadores de presión, actuadores como por ejemplo controles y sistemas de control de robot, sistemas de campo de E/S como acopladores de fieldbus, Interfaces Hombre-Maquina (HMI) como paneles de PC's son integradas por mencionar unas pocas del amplio rango de posibilidades. Adicionalmente la red puede ser conectada a Internet para habilitar el acceso basado en Web para controlar dispositivos por razones de mantenimiento. También el set de uso de los protocolos de comunicación basados en Ethernet es mas largo que en el campo de la oficina.

Como se indico anteriormente el set de protocolos de Internet como FTP, HTTP, SNMP, DHCP y otros más esta extendido con protocolos de automatización como son EtherNet/IP, Modbus TCP, Ethernet Powerlink, SERCOS III y EtherCat. Estos protocolos de comunicación están dedicados a llenar requerimientos especiales de las interacciones individuales de los dispositivos de automatización. Por lo tanto estos habilitan una desviación desde el paradigma cliente-servidor para habilitar la transmisión de datos entre mas de dos parejas de  de comunicación como es el caso de los paradigmas publish-suscribe y productor-consumidor.

El tamaño de los datos transmitidos entre dispositivos varía desde un par de bytes como es el caso de una comunicación entre un PLC y una E/S de campo hasta algunos cientos de megabytes para el caso de una comunicación entre un sistema de control CNC y su dispositivo de programación.

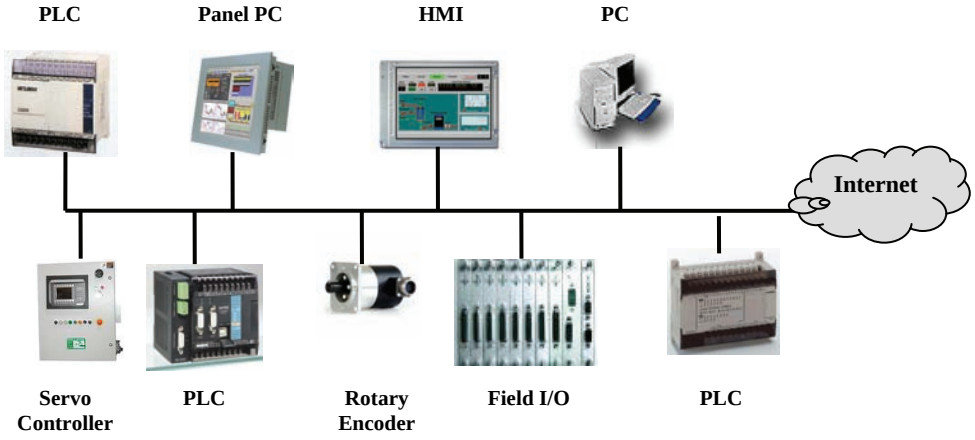



***Figura 2-11 Ejemplo de una red industrial***

Se puede ver en forma general que en las parejas de comunicación dentro de las redes de comunicación tanto en oficinas como en fábricas las constantes de tiempo de los sistemas de comunicación en ambos campos difieren significativamente. La duración de las interacciones de comunicación y el nivel necesario de sincronismo es mucho mayor en la fábrica que en la oficina.
Dentro de la oficina no es relevante si un archivo PDF es transmitido en 2 o 4 segundos desde la PC a la impresora o si desplegar una pagina Web tarda 1 o 5 segundos. También una variación de la velocidad de comunicación es solo de limitada relevancia. En cualquier caso las actividades necesarias pueden ser hechas apropiadamente y una situación de daño o falla no ocurrirá.

En contraste con esto, en la fábrica la principal importancia en cuan rápido las señales de un actuador conseguirán accionar un controlador y que tan rápido los comandos de control resultantes serán transmitidos a los actuadores. Aquí, un tiempo de procesamiento de aplicación a aplicación de unos pocos milisegundos o aun unos pocos microsegundos pueden ser necesarios para evitar situaciones peligrosas las cuales pueden ocurrir si por ejemplo, un sistema de movimiento lineal se moviera de su posición final o una alta tensión excesiva de una membrana de papel no fuera reconocida en una maquina de impresión.
Adicionalmente, el sistema de comunicación tiene que asegurarse que la fluctuación durante la transmisión de datos sea pequeña. Para proveer estas características, una sistema de comunicación basado en Ethernet para la fabrica tiene que ser tan rápido y deterministico como sea posible, especialmente mas rápido en algunas magnitudes y mas deterministico que en el mundo de la oficina.

Otra importante diferencia entre los sistemas de comunicación de oficina basados en Ethernet y sistemas de comunicación basados en Ethernet a nivel industrial son los diferentes requerimientos en la estabilidad del sistema. Fallas dentro de una red de oficina puede resultar en destrucción de archivos de datos y algunas veces conexiones de comunicación rotas. Tales fallas son un fastidio para los empleados dentro de la oficina afectada desde el tiempo que se requerirá para la recuperación de los archivos perdidos y una reinstalación o un reinicio de los links de comunicación y los componentes activos de red. Pero dentro de una red industrial una falla en el sistema de comunicación resultara en problemas mas fuertes y puede generar situaciones peligrosas para empleados y maquinaria así como para el entorno. Un pequeño problema pueda causar una falla del sistema y esto se traducirá en para el sistema de producción por un cierto periodo de tiempo. El principal problema son los posibles daños de la maquinaria, sistemas de transporte y piezas de trabajo las cuales resultaran en un retraso o en pérdida de información crítica. Aquí, los costos de algunos millones de pesos, dólares o Euros son posibles.

Para arreglárselas con este problema de estabilidad los sistemas de comunicación basados en Ethernet tienen que contener un mecanismo de seguridad de estructura y de naturaleza tecnológica.
Las fallas de comunicación son resultado de influencias mecánicas, térmicas, o electromagnéticas y tienen que ser evitadas o manejadas con el uso de tecnologías de cableado apropiadas y topologías como cable blindado o cableado redundante. Fallas de comunicación resultantes de las propiedades técnicas y de las tecnologías usadas dentro de los sistemas basados en Ethernet como la aplicación de la tecnología CSMA/CD para acceder al medio de comunicación hace cumplir la consideración de las combinaciones apropiadas de condiciones estructurales y dispositivos adecuados como la combinación de comunicación full-duplex y switches además de la limitación de la carga del sistema de comunicación al 10% de la carga máxima que el sistema puede soportar.

Adicionalmente al problema de estabilidad también el problema de la seguridad tiene que ser cuidado usando una apropiada infraestructura y topología del sistema de comunicación. Conectar a sistemas de comunicación basados en Ethernet desde la Internet todos los dispositivos es teóricamente accesible desde fuera de la industria. De ese modo, las compuertas están abiertas para hackers.
Por lo tanto, las tecnologías de seguridad necesarias y mecanismos como firewalls y permisos de acceso tienen que ser consideradas dentro de cada sistema de comunicación industrial basado en Ethernet. Esto tiene que ser realizado adaptándose a los objetivos del sistema de comunicación industrial y por lo tanto no debería influenciar las propiedades del tiempo real de la comunicación.

La dimensión de la seguridad de las personas y los problemas de seguridad se incrementaran con la integración de nuevas tecnologías dentro de redes Ethernet dando nuevos beneficios y desventajas. Por ejemplo la tecnología Wireless Ethernet mejorara la flexibilidad de las redes con respecto a demasiados dispositivos integrados pero en suma puede darse un fácil acceso desde fuera si no es usado en una vía segura. Otro ejemplo es el cableado de fibra óptica. Este tipo de cable reducirá la influencia de radiación electromagnética al mínimo pero requiere más destrezas dentro de la fase de instalación.

Lo ultimo pero no menos importante es la manejabilidad al usuario que tiene que ser mencionada. En el caso de la aplicación final de un sistema de comunicación industrial no puede ser ocultado que cada trabajador implementando, usando o manteniendo el sistema de comunicación tiene un conocimiento acerca de los fundamentos técnicos y especializados del sistema basado en Ethernet, el protocolo TCP/IP, y otros protocolos de alto nivel usados desde el lado de Internet o del lado de la fabrica. Por ejemplo los detalles internos de la distribución de direcciones en el protocolo DHCP, la estructura de la petición de lista de identidades dentro del protocolo Ethernet/IP, o la parametrización de un firewall especial será un conocimiento adquirido por fuera para la aplicación en la planta industrial. Por lo tanto, el diseño, implementación y aplicación tiene que ser soportada por herramientas fáciles de usar y una guía de usuario suficiente.
Sumando las principales diferencias entre las comunicaciones de oficina y los sistemas de comunicación a nivel industrial pueden ser encontrados dentro del campo de las influencias ambientales en el sistema de comunicación, la velocidad de la comunicación y la predictibilidad, datos transmitidos del usuario, protección del sistema y estabilidad, consecuencias de las fallas y conocimiento del usuario. Estos hechos están agregados en la siguiente tabla:

| | Oficina | Fabrica |
|---|---|---|
| Entorno | Oficina Limpia | Fumar, polvo, humedad, agua, mugre, campos electromagnéticos, etc. |
| Usuario | Trabajador de mantenimiento especializado | Trabajador parcialmente calificado. |
| Tiempos de Reacción | Segundos | Menor a Microsegundos |
| Disparo | Segundos | Menor a Microsegundos |
| Tamaño de Datos | Hasta MB | Cuando menos 1 bit |
| Protección | IP 20 / IP 54 | IP 20 in cabinet / IP 67 in field |
| Posibles consecuencias de fallas | Perdida de datos o de producción | Perdida de datos, de producción, daño a maquinas, riesgo a humanos & entorno |

***Tabla 2-3 Polvo y Humedad – los principales problemas de los sistemas de comunicación industrial***

## 2.3 Cableado en la industria

La aplicación de los sistemas de comunicación basados en Ethernet requiere la creación de un sistema de cableado como en el caso de los sistemas fieldbus.
Desde el – con respecto a los sistemas de comunicación industrial – desde el punto de vista amateur de un usuario de oficina, el cableado Ethernet es simplemente conectar diferentes tipos de hubs, switches y dispositivos juntos con cable apropiado y conectores usando la instalación Ethernet del edificio.
Pero este punto de vista descuida los problemas esenciales resultado de la consideración necesaria del trafico entre dispositivos, diferentes tipos de cables, conectores y otros componentes, la tasa de transmisión aplicable, situaciones del entorno, etc. Además, las aplicaciones industriales requieren la consideración de la integridad de los datos, la seguridad de los mismos, redundancia y más.
Las consideraciones adicionales mencionadas están mostrando la brecha que emerge entre la aplicación de sistemas basados en Ethernet dentro del mundo de la oficina y la aplicación dentro de diferentes entornos a nivel industrial.

Para una instalación exitosa de un sistema de cableado Ethernet en general se siguen 4 etapas que son necesarias, estas son:

1. **La fase de especificación:** Dentro de esta fase los requerimientos detallados para el cableado como son: su acomodo y los servicios asociados a la instalación direccionando los entorno(s) específicos son identificados dentro de las premisas para ser aplicadas juntas con el aseguramiento de calidad necesarios. Basados en los requerimientos de la topología especifica, componentes aplicados y trayectorias de uso de cable serán seleccionadas.

2. **La fase de implementación:** Dentro de esta fase la instalación física en acuerdo con los requerimientos de la especificación es hecha.

3. **La fase de inicio:** Dentro de esta fase el sistema implementado será probado con respecto a los requerimientos definidos en la fase de especificación. Las pruebas serán documentadas.

4. **La fase de operación:** Dentro de esta fase el manejo de conexiones y el mantenimiento del rendimiento de la transmisión es hecho a través del ciclo de vida del sistema de cableado.

El problema principal de la fase 1 es definir la topología del sistema. La topología usual en un sistema de comunicación en oficina definida en los estándares internacionales ISO/IEC 11801 y EN 50173 siguen una topología en estrella multinivel. Un edificio contendrá al menos un distribuidor de edificio. Todos los distribuidores de edificio dentro de un campus serán conectados a un distribuidor de campo. Estos distribuidores de campo serán el punto de comunicación central del área completa y aseguraran la conexión a la Internet.
Dentro de un edificio usualmente existen varios distribuidores de piso. Estos distribuidores acoplarán terminales de salida, por ejemplo: PC's de oficina, impresoras, etc.
Las consideraciones dentro de los entornos industriales han mostrado que esta estructura general puede ser también aplicada a los sistemas de comunicación Ethernet. Por lo tanto, la descripción de la topología dentro de la guía será basada en esta estructura, solo cambios menores son necesarios. Hay diferencias entre la oficina y las aplicaciones industriales debido a la dimensión de la red, redundancia y capacidades de tiempo real requeridas. Básicamente una industria puede compararse con un edificio. Claramente, este punto de vista es ligeramente distinto al punto de vista de la oficina por razones de la dimensión del sistema, sin embargo, las estructuras resultantes son semejantes.
Por lo tanto, la topología dada en el estándar ISO/IEC 11801 será extendido por una maquina distribuidora (o distribuidor) el cual puede compararse al distribuidor industrial.

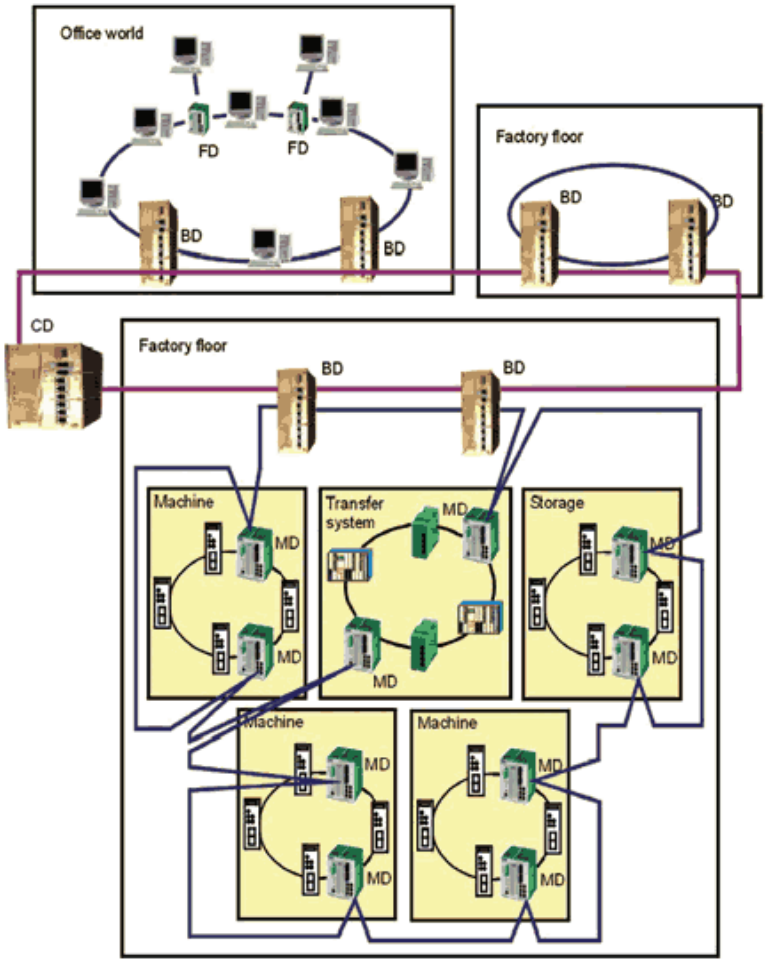



***Figura 2-12 Topología básica para un sistema de cableado Ethernet industrial***

La topología resultante basada en los cuatro diferentes niveles de distribuidor de campo, distribuidor de edificio, distribuidor de piso y maquina distribuidora dependen de los requerimientos de redundancia, esfuerzo del cable y otros. Aquí las topologías de estrella, topologías de bus tan buenas como las topologías de anillo pueden ser utilizadas.
Especialmente en el entorno industrial la topología de anillo parece ser la más adecuada desde que hizo posible la redundancia con un esfuerzo mínimo del cable. Por lo tanto para una red de comunicaciones industriales Ethernet la topología de anillo jerárquica entrelazada será la topología mas usada.

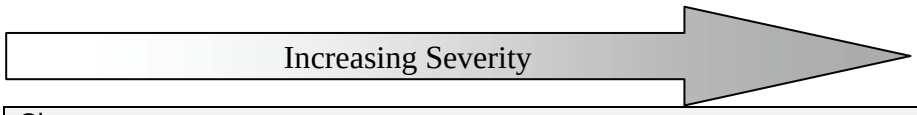
Cada topología de red resultara en una serie de requerimientos con respecto a la tecnología de la red y los componentes. Un conjunto de dispositivos distintos y componentes de infraestructura pueden ser usados para diferentes propósitos y para diferentes necesidades. Esto incluye diferentes componentes pasivos como conectores y cables así como componentes activos como son los hubs, switches y gateways. Estos componentes tienen que ser seleccionados apropiadamente para asegurar completamente la especificación del comportamiento del sistema. La selección de los componentes se decidirá acerca de la protección contra las influencias ambientales, tasas de datos usables, posibles canales de comunicación, etc.

Los estándares de cableado general para componentes pasivos están descritos de acuerdo a sus propiedades. Pero el uso del estándar de la tecnología de oficina dentro de los entornos industriales es imposible.

Los requerimientos adicionales para el entorno industrial resultado del polvo, humedad del aire, estrés mecánico, altas temperaturas y otros esta reflejado en por dos clases de componentes los cuales tienen diferentes características con respecto a la instalación. Componentes de "función ligera" o "Light Duty" serán aplicados dentro de tableros industriales o tarjetas de switches, donde los componentes de "función pesada" o "Heavy Duty" serán aplicados en áreas industriales sin protección. La opción de componentes individuales depende del nivel de influencias externas en las que los mismos tienen que arreglárselas. En consecuencia de esta distinción diferentes tipos de cables especiales a partir de la Categoría 5 y mayores tan bien como diferentes tipos de conectores para llenar los requerimientos existentes IP20 e IP67.

Para la descripción de los entornos el grupo de trabajo ISO/IEC llamado IPTG y el grupo CENELEC llamado PTIP han sugerido una descripción extendida de las clases de entornos. Aquí una combinación de 3 categorías para influencias ambientales con 4 categorías (influencias mecánicas, térmicas, electromagnéticas y clases IP) es descrita. La matriz resultante permite el diseño del sistema de comunicación para seleccionar el mejor camino para seleccionar los mejores componentes del sistema de cableado.

Dentro de esta matriz de clasificación la combinación de clases M1I1C1E1 se posiciona como el principal dentro de las redes de oficina en un contenedor de oficina, M3I1C1E1 permanece para las subredes dentro de un recinto adecuado en la industria y el M3I3C3E3 esta para una subred dentro de un campo no protegido del polvo, alta humedad, etc.




| | Classes | | |
|---|---|---|---|
| Mechanical | $M_1$ | $M_2$ | $M_3$ |
| IP Rating | $I_1$(IP20) | $I_2$ | $I_3$(IP67) |
| Climatic | $C_1$ | $C_2$ | $C_3$ |
| Electro-magnetic | $E_1$ | $E_2$ | $E_3$ |

***Tabla 2-4 Tabla MICE resultado de las actividades de estandarización IEC/ISO y SEMELEC***

Los componentes activos serán considerados con respecto a su función dentro de las diferentes capas de la red, (por ejemplo una maquina distribuidora y un distribuidor de edificio) y los tiempos de respuesta requeridos. Basado en suposiciones acerca de los dispositivos finales Ethernet conectados (PC's, estaciones de trabajo, PLC's, dispositivos de E/S, etc.) y en las aplicaciones que probablemente serán usadas en ellos en los años siguientes, uno tiene que calcular las probabilidades de trafico para cada link en la red planeada. Eso no es suficiente para calcular la carga promedio, los picos de carga también tienen que ser estimados para así evitar sobrecargas temporales de la red.
La mayoría de aplicaciones de oficina son tolerantes acerca de la entrega o las variaciones en los tiempos de respuesta.
Pero en los sistemas de control y aquí, por ejemplo, los sistemas de control de movimiento o sistemas de control de seguridad tienen restricciones muy fuertes en sus tiempos de respuesta. Los segmentos relevantes que llevan paquetes de comunicación de tiempo real deberían ser mantenidos libres de cualquier trafico innecesario dimensionados con al menos un factor de 10 del ancho de banda reservado.

Un incremento en el manejo de la carga de tareas traseras (background load) es esperado los procesos de control y automatización discreta – pero esto será siempre en picos temporales y sin requerimientos rigurosos en el tiempo de respuesta –. Esto puede ser manejado fácilmente por un switch de red con prioridades de tráfico.

Después del diseño y la planeación, el siguiente paso es la instalación. Para una instalación profesional, en esta etapa, los diferentes problemas emergen de los distintos tipos usables de material de cableado y especialmente los diferentes tipos de cable tienen que ser considerados seriamente.
Principalmente los dos diferentes tipos de cable “cable de fibra óptica” y “cable de cobre” tienen que ser distinguidos con respecto a las dos clases de entorno “Light Duty” o “Heavy Duty” o con respecto a la tabla MICE. En el caso de la configuración de la conexión del cableado de cobre, la distancia mínima a fuentes de interferencia siguiendo la clasificación dentro del estándar IEEE 518-1982 dentro o fuera de recintos, estrés mecánico, interferencias electromagnéticas, el conductor debe ser revisado en todas sus características para poder ser considerado.
En el caso de cables de fibra óptica la interfaz, el tipo, capacidades de los cables usados y la calidad de la instalación además de la configuración de conexión requieren de atención. En suma a los problemas considerados con respecto a los tipos de cable también la definición de las trayectorias de estos, el etiquetado de los cables y la documentación del cableado son muy importantes.

Para garantizar fiabilidad y comportamiento apropiado, es necesario probar el sistema de cableado como se describe en el estándar ISO/IEC 11801. Para pruebas de cableado de cobre en el mapeo de líneas pueden ser aplicadas resistencia DC en bucle (DC loop resistance), largo del cable, atenuación, diafonía cercana al fin del bus (near-end crosstalk) y punto de conexión pueden ser aplicados.
Para cableado de fibra óptica los diferentes modos de transmisión de datos, pérdida de presupuesto y herramientas de pruebas básicas, perdida de potencia y OTDR deberían ser considerados.

## 2.4 Estructuras de comunicación

Como se mencionó en el capitulo anterior los sistemas basados en comunicaciones Ethernet pueden seguir diferentes estructuras. Esto es valido para estructuras físicas en la topología o así como para estructuras lógicas de las conexiones de comunicación. Aquí diferentes términos como topología de anillo o estrella, unicast o multicast, o principios como editor-suscriptor o productor-consumidor pueden ser encontrados. Dentro de este subcapítulo los diferentes términos serán descritos dentro del contexto de una comunicación industrial basada en Ethernet.

### 2.4.1 Topologías físicas

Comenzando con la tecnología 10BaseT de dos líneas de par trenzado llamada de pares trenzados ha llegado está a ser el estándar de cableado para los sistemas de comunicación basados en Ethernet. Ahora las fibras ópticas están viniendo a reemplazar parcialmente el cableado de par trenzado especialmente en los backbones (columnas vertebrales). Ambas tecnologías la de par trenzado y la de fibra óptica demandan la misma topología física. En ambos casos en general un link de comunicación (por ejemplo un cable) conectará a una pareja de aparatos usando una tarjeta de red (lógica) dentro de cada uno el cual es físicamente conectado al link de comunicación. Esto se representa en la figura siguiente.

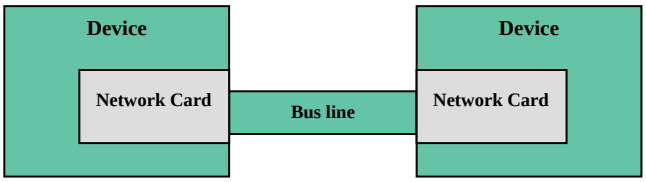



***Figura 2-13 Topología física básica de un sistema de comunicación Ethernet desde 10BaseT***

Dentro de esta topología básica no es relevante si alguno de la pareja de comunicación tiene dispositivos de control u otros dispositivos terminales o si ellos son componentes activos del sistema de comunicación como switches o hubs. La estructura de conectar dos dispositivos con un cable de link es la misma.

Basados en esta topología básica dos principales topologías de red básicas pueden ser definidas.
La primera es la de línea o topología de anillo. (Un anillo tiene que ser considerado una línea cerrada desde el punto de vista físico). Para esta topología se tiene que asumir que cada pareja de comunicación esta equipada con al menos dos tarjeta de red. Entonces, las parejas de comunicación estarán conectadas en una fila o hilera conectando los dispositivos uno por uno. Un set de datos será enviado dentro de esta estructura siguiendo la línea de los dispositivos desde el dispositivo transmisor hasta el dispositivo receptor del mensaje conteniendo los datos.

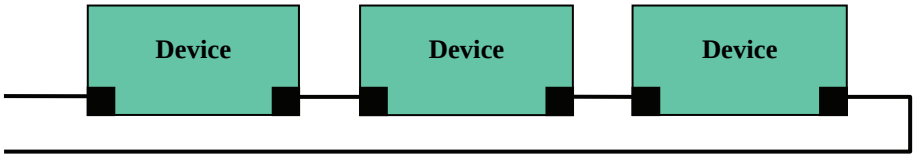



***Figura 2-14 Topología física en línea/anillo***

La segunda topología básica es la topología de estrella. Esta requiere componentes activos adicionales como switches y hubs. Estos componentes activos pueden ser considerados como un set de tarjetas de red, los cuales están internamente conectados con cierta lógica.
Cada dispositivo estará conectado con un cable a un hub/switch y se comunicara utilizando este dispositivo como transmisor. Un set de datos entrantes a una de las tarjetas de red será reenviado usando uno o un set de otras tarjetas de red.

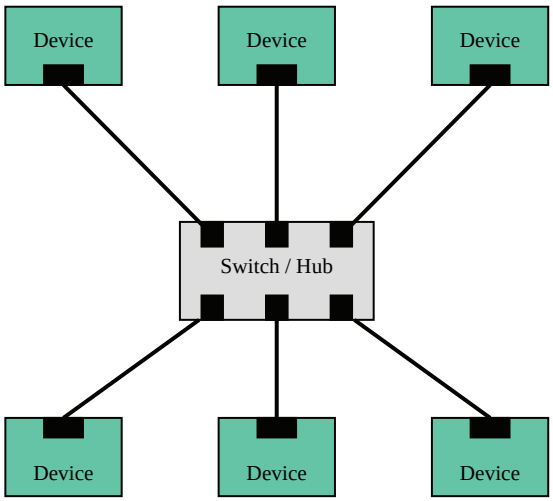



***Figura 2-15 Topología física en Estrella***

De este modo los switches se distinguen de los hubs por su funcionalidad de filtrado la cual no se proporciona en un hub. Un hub reenviara un mensaje entrante a todas las tarjetas de la red las cuales son diferentes de la tarjeta de red receptora y del destino del mensaje. Dentro de un switch el destino de un mensaje será determinado. Dependiente del destino del mensaje (un mensaje broadcast o multicast tiene mas de un destino) solo las tarjetas de red serán usadas para reenviar el mensaje teniendo por lo menos un destino.

Naturalmente, ambas topologías básicas pueden ser combinadas para conseguir topologías más complejas. Usualmente las topologías consisten en estrellas interconectadas, anillos interconectados, o combinaciones de ambos son aplicables. Dentro del mundo de la oficina la topología de estrella interconectada basada en las normas estándar ISO/IEC 11801 y EN 50173 es la más utilizada.

En la industria la topología mas utilizada es una interconexión organizada jerárquicamente de diferentes anillos. Una versión especial de la combinación de ambas topologías es la llamada topología Daisy Chain.

Esta topología recibe un creciente interés en la automatización industrial desde que esta redujo los esfuerzos del cableado por evitar componentes activos. La topología Daisy Chain es teóricamente una topología que consiste en estrellas triples interconectadas en una cadena.
Pero en la práctica los componentes activos necesarios están integrados dentro de los dispositivos. Así una línea virtual o topología de anillo es generada.

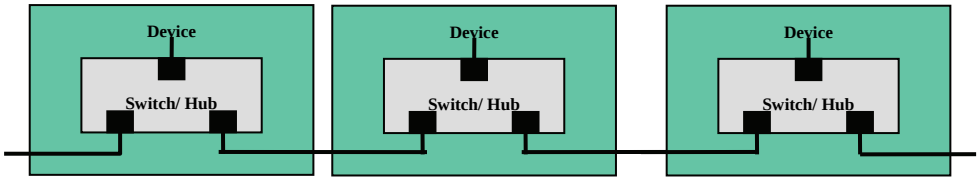



*Figura 2-16 Topología Daisy Chain*

### 2.4.2 Topologías lógicas

La topología lógica de un sistema de comunicación basado en Ethernet es la más grandemente extendida independiente de la topología física. En su mayoría, la topología lógica es considerada como una topología de bus. Esto implica que cada pareja de comunicación es apta para enviar un mensaje a cada otra pareja de comunicación pero todas las parejas pueden observar esta comunicación.

Este hecho fundamental tiene una limitación por la aplicación de switches. Desde que los switches reenvían mensajes solo a un subset de tarjetas de red salientes todas las parejas de residentes de tarjetas no usadas son excluidas de la comunicación especial.

El concepto de mensajes broadcast, multicast y unicast han estado establecidos con el fin de distinguir entre mensajes los cuales pueden observados por todas las parejas de comunicación y mensajes reservados solo para algunos o una pareja de comunicación para la aplicación de una red completamente switcheada.

Mensajes broadcast son transmitidos a cada pareja de comunicación y están caracterizados por una dirección IP especial a un nivel IP dependiendo de la red y la definición de la mascara de subred. Un dispositivo con la dirección IP local 192.168.10.26 y la mascara de subred 255.255.255.0 conseguirá todos los dispositivos dentro del rango IP 192.168.10.1 – 192.168.10.254 enviando un mensaje a la dirección IP multicast 192.168.10.255.

En un nivel Ethernet esta dirección multicast es igual a la dirección MAC ff:ff:ff:ff:ff:ff.
Utilizando mensajes broadcast se habilita la aplicación de una topología lógica.
El uso de mensajes unicast como el opuesto posibilita la aplicación de una topología lógica donde cada pareja de comunicación esta directa y exclusivamente conectada con todas las demás parejas de comunicación. Un dispositivo con la dirección IP local 192.168.10.26 y la mascara de subred 255.255.255.0 conseguirá al dispositivo con la dirección IP 192.168.10.83 por medio del envío de un mensaje a esa dirección. Los demás dispositivos no recibirán ese mensaje desde que los switches ruteen el mensaje solo al receptor. La próxima topología lógica es una topología grafica completa teniendo arcos directos entre las posibles parejas de comunicación.

Los mensajes multicast tienen un poco de los mensajes broadcast y unicast. Un mensaje multicast será recibido por un set de receptores pertenecientes a un grupo multicast. Un grupo multicast es caracterizado por su dirección IP multicast. Esta dirección esta dentro del rango de direcciones 224.0.0.0 – 239.255.255.255. Pero algunas de estas direcciones están reservadas para propósitos o servicios especiales. Para el ruteo de mensajes multicast dentro de un grupo todos los dispositivos con funcionalidad de ruteo extenderán un árbol de ruteo sobre la red.

Para unir este árbol y de este modo conseguir todos los mensajes multicast de un grupo multicast un dispositivo tiene que enviar un mensaje especial IGMP (Internet Group Management Protocol) en la red. Claramente un dispositivo puede pertenecer a un grupo o a más grupos multicast incluso a ninguno. En el nivel Ethernet el mapeo de direcciones IP multicast a direcciones MAC no es único. Esto es debido al espacio de direcciones más pequeño para multicast en el nivel Ethernet.
Por ejemplo las direcciones IP 224.128.64.32 y 224.0.64.32 ambas serán mapeadas a la dirección MAC 01:00:5e:00:40:20.
Por lo tanto, en el nivel de implementación de los dispositivos tiene que aplicarse un funcionalidad de filtrado. Pero de cualquier manera, la aplicación de mensajes multicast posibilita una topología lógica basada en un bosque de árboles dentro de la red.

### 2.4.3 Estructuras de comunicación basadas en interacciones

La comunicación basada en interacciones parejas de comunicación individuales es de nuevo la gran posible extensión independiente de la física así como de la topología lógica del sistema de comunicación. Las estructuras de comunicación están relacionadas al camino de comunicación en el que las parejas de comunicación solicitaran y proveerán datos, así como a la vía que fija los datos individuales que son intercambiados durante la petición de datos y el procedimiento de provisión.
Actualmente, tres estructuras de interacción muy importantes pueden ser observadas.

Estas son la estructura Cliente-Servidor, la estructura Editor-Suscriptor (Publish-Subscribe) y la estructura Productor-Consumidor. Todas estas estructuras importantes tienen sus pros y contras individuales y de ese modo difieren con respecto a la aplicabilidad de ciertos problemas.

La estructura Cliente-Servidor es principalmente aplicada en el caso de un intercambio de datos entre solo una pareja de comunicación. En este caso ningún otro dispositivo requiere también del intercambio de datos. Usualmente el cliente, es decir el socio de comunicación requiriendo los datos los cuales pueden ser provistos por el otro socio (el servidor), comienza la interacción enviando un mensaje apropiado de solicitud al servidor. Su propósito es forzar al servidor a hacer una actividad especial la cual contiene los datos procesados y transmitidos, los datos de preparación y respuesta, o ambos. Si el servidor recibe el mensaje de solicitud del cliente éste hace la acción solicitada y envía un mensaje de respuesta conteniendo (tal vez) los datos solicitados. Después de una solicitud y un mensaje de respuesta la interacción es finalizada. La estructura Cliente-Servidor es usualmente implementada para mensajes unicast. Un ejemplo prominente pero no único de esta estructura es el protocolo Modbus/TCP.

La estructura Cliente-Servidor provee una eficiente estructura de interacción para intercambio de datos explícitos entre exactamente dos socios de comunicación como dos dispositivos de control (posiblemente PLC's). En el caso de sensores de datos, los cuales tienen que ser intercambiados entre un codificador giratorio y un PLC en un modo cíclico, esta estructura no es eficiente.

Dentro de cada ciclo, esta estructura requiere una solicitud la cual de hecho no es necesaria. Si más de un dispositivo de control requiere los datos del sensor del codificador giratorio el problema aumentara. Aquí cada socio interesado tiene que enviar una solicitud y tendrá una respuesta. De ese modo, la carga del sistema de comunicación se incrementara significativamente.

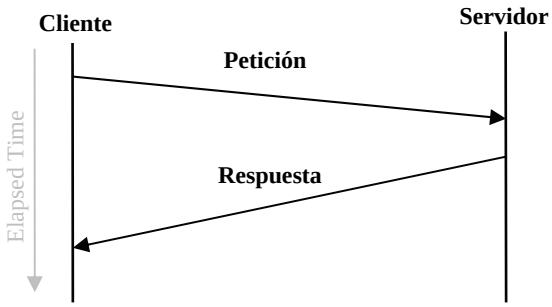



***Figura 2-17 Diagrama de mensaje de una estructura Cliente-Servidor***

Para evitar estos problemas dos estructuras de interacción han sido diseñadas para reducir los mensajes de solicitud a un numero mínimo y posibilitando la aplicación de un mensaje de respuesta a todos los interesados. Claramente, estas estructuras están caracterizadas por el movimiento aplicado de mensajes de unicast a multicast para los mensajes de respuesta además de la adición de socios de comunicación que requieren los mismos sets de datos dentro de grupos. Estas estructuras de interacción son la estructura Editor-Suscriptor (Publisher-Subscriber) y Productor-Consumidor (Producer-Consumer).

Dentro de la estructura Editor-Suscriptor el set de socios de comunicación destinados a recibir el mismo set de datos y por lo tanto pertenecer a un grupo es guardado y mantenido por el Editor (Publisher), es decir el socio de comunicación teniendo los datos de interés. Cada pareja de comunicación del grupo mencionado enviara una solicitud al editor indicándose el mismo como un suscriptor de los datos de interés. El editor integrará al nuevo suscriptor en su lista de suscriptores y enviara cíclicamente los datos a todos los miembros de su lista de suscriptores. Esto se hace enviando un mensaje multicast.

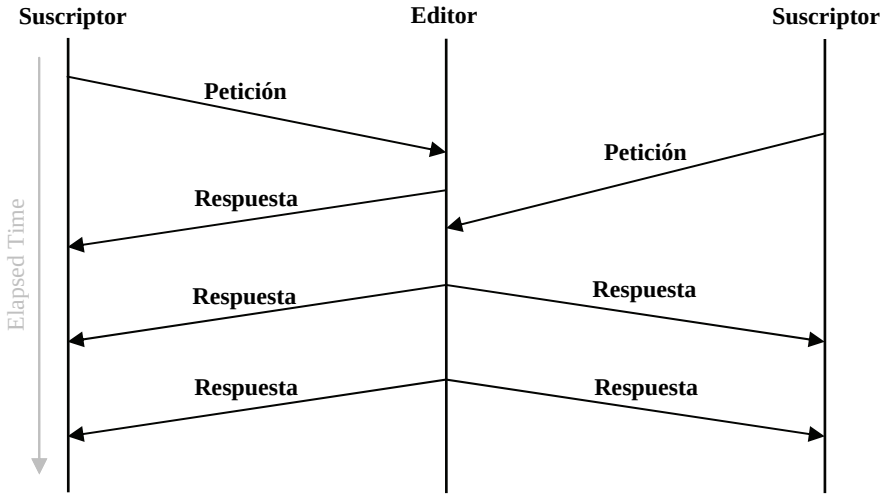



***Figura 2-18 Diagrama de mensaje de una estructura Publish-Subscriber***

Dentro de las implementaciones especiales la aplicación de mensajes multicast no es mandataria. En el caso de pequeños sets de suscriptores el editor puede también enviar mensajes unicast a todos los miembros del set de suscriptores. En este caso el envío de mensajes a todos los suscriptores es hecho en el mismo momento o al menos tan rápido como es posible en una secuencia. Esto reducirá los esfuerzos de mantenimiento del grupo suscriptor dentro del editor.

Dentro de la estructura Productor-Consumidor los sets de datos también son transmitidos vía mensajes multicast. En contraste a la estructura Editor-Suscriptor, dentro de la estructura Productor-Consumidor los socios de los grupos de comunicación los cuales están interesados en los mismos sets de datos no son mantenidos por un socio de comunicación.

Para habilitar a los socios de un grupo de comunicación cada set de datos es etiquetado por un identificador especial de comunicación. El primer consumidor de un set de datos esta enviando una petición al productor de los datos. Juntos, el productor y el primer consumidor negociaran una dirección multicast además de un identificador de comunicación para los mensajes conteniendo el set de datos de interés.

El productor empezara a enviar el set de datos a las direcciones multicast definidas. Si otro consumidor esta interesado en el mismo set de datos éste solicitara la dirección multicast y el identificador de comunicación desde el productor u otro consumidor y puede entonces empezar a filtrar los mensajes con el set de datos de interés desde el set de los mensajes multicast transmitidos.

Como se menciono antes, el proceso de ingreso y abandono para un grupo multicast productor-consumidor es manejado por los mensajes IGMP. Un buen ejemplo de la implementación de la estructura Productor-Consumidor es el protocolo EtherNet/IP.

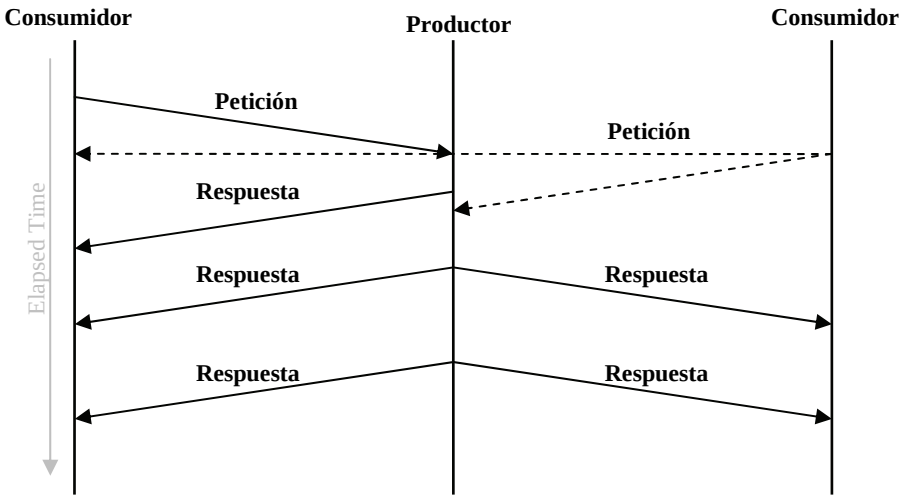



***Figura 2-19 Diagrama de mensaje de una estructura Productor-Consumidor***

Ambas estructuras, Productor-Consumidor y Editor-Suscriptor reducen la carga de un sistema de comunicación basado en Ethernet. Pero estos requieren también capacidades adicionales de los dispositivos integrados en el sistema de comunicación con respecto a la transmisión y recepción de mensajes multicast o broadcast los cuales no es dado por ningún dispositivo.

## 2.5 Seguridad de red

Con el crecimiento de las redes de producción y redes de oficina, la seguridad de red representa uno de los asuntos más importantes cuando se utiliza Ethernet en un entorno industrial. Los datos son proporcionados por amplios sectores en la corporación, diferentes sucursales son conectadas usando la Internet como una WAN (Wide Area Network) muy barata la cual esta conectada a una red corporativa virtual. De este modo, este capitulo da una introducción a los pasos básicos en la planeación de la seguridad de la red para un entorno Ethernet industrial.

### 2.5.1 Términos y definiciones

El primer paso en el reto de la seguridad de red forma la definición de los términos básicos para definir lo que “seguridad” significa. Esto no esta dedicado a definiciones sólidas, mas bien muestra los cinco términos básicos para en criterios de seguridad que una red debería ofrecer:

- **Integridad:** Los datos transmitidos no serán modificados en la trayectoria de transmisión, estarán completos, y alcanzaran su objetivo (dirección/es) en el mismo orden como fueron transmitidos por el emisor. Por ejemplo, los datos de un archivo de transferencia FTP no son intercambiados con una tercera persona durante la transmisión.

- **No-repudiabilidad**: Esto puede ser verificado en cualquier tiempo por quien ha iniciado una conexión y quien ha transmitido cuales datos en que punto en el tiempo. En la practica esto significa, por ejemplo que los datos de los archivos de acceso (log files) son explícitos y resistentes al fraude. Esto es especialmente útil para escenarios de mantenimiento remoto donde los fabricantes acceden a sus componentes en una instalación existente, por ejemplo para actualizar software. En caso de falla de la instalación causada por estas actividades de mantenimiento el fabricante puede verificar el nivel de responsabilidad basado en los archivos de acceso (log files) resistentes a fraudes.

- **Confidencialidad**: Los datos enviados no pueden ser accedidos por una tercera persona en la trayectoria de transmisión. Por ejemplo, este objetivo puede ser conseguido usando algoritmos criptográficos apropiados que extienden lo que ellos pueden aplicar. La aplicación de dichos algoritmos puede ser problemática debido al alto grado de capacidades de procesamiento necesarias, especialmente con respecto a la comunicación en tiempo real y a los dispositivos on-board con las restricciones de CPU respectivas.

- **Disponibilidad**: La red y dispositivos conectados pueden enviar y procesar datos en cualquier momento dentro de un cierto marco de tiempo dado. La disponibilidad forma un punto muy intratable en relación con la seguridad de red en sistemas de automatización. Como resultado de la restricción de recursos de los sistemas on-board (incrustados) el acceso a estos dispositivos puede ser prevenido sobrecargando la red (negación del servicio).

- **Autenticación**: Durante el proceso de autenticación, la identidad de un socio en la comunicación es determinada y adicionalmente es checada, si este socio tiene los derechos de acceso requeridos para un servicio de red dado. En la práctica, la combinación Usuario/Contraseña (por ejemplo para una transferencia FTP) o la firma digital (por ejemplo para la comunicación por e-mail) cae en esta categoría.

Basados en estos criterios los llamados objetivos de protección uno puede definir contra cual red tiene que ser protegido:

- Protección contra **obtención de información no autorizada** (perdida de confidencialidad)
- Protección contra **modificación de información no autorizada** (perdida de integridad)
- Protección contra **interferencia de funcionalidad no autorizada** (perdida de disponibilidad)

### 2.5.2 Flujos de la familia de protocolos IP

Nadie puede dudar que la familia de protocolos IP es muy potente. Los enormes montos de datos los cuales se transfieren sobre la Internet día con día muestra su flexibilidad y estabilidad. Pero ahí también hay algunos diseños de flujo los cuales pueden causar problemas relacionados a la seguridad. Algunos de estos flujos serán descritos más adelante con más detalle.
La siguiente sección discutirá algunos problemas concretos a fondo de la familia de protocolos IP y como estos problemas pueden ser usados para evitar entrar en mecanismos de seguridad.

Un primer planteamiento para evitar el masquerading y mecanismos de ruteo es falsificar la dirección fuente de un paquete IP, conocido como engaño IP (IP spoofing). El paquete con la dirección falsa aparece en la tarjeta del ruteador de la red conectado a la Internet y el ruteo envía este paquete a la tarjeta de red interna. De esta forma se puede crear tráfico de red dentro en la Intranet y por esto la causa parece originarse desde la red local. Este problema es ejecutado por el llamado Source Routing del protocolo IP. IP ofrece la posibilidad de especificar la ruta completa de un paquete al destino en la cabecera IP. Una implementación corrupta del router puede remitir normalmente un paquete no ruteable al destino sin checar que la dirección fuente es imposible.
Esto tiene que ser mencionado ya que algunos grandes proveedores de Internet siguen permitiendo el IP spoofing así que esto es un problema actual. El reconocimiento de paquetes falsos desde la Intranet es mucho más difícil debido a que el supuesto creador puede ser el creador real.

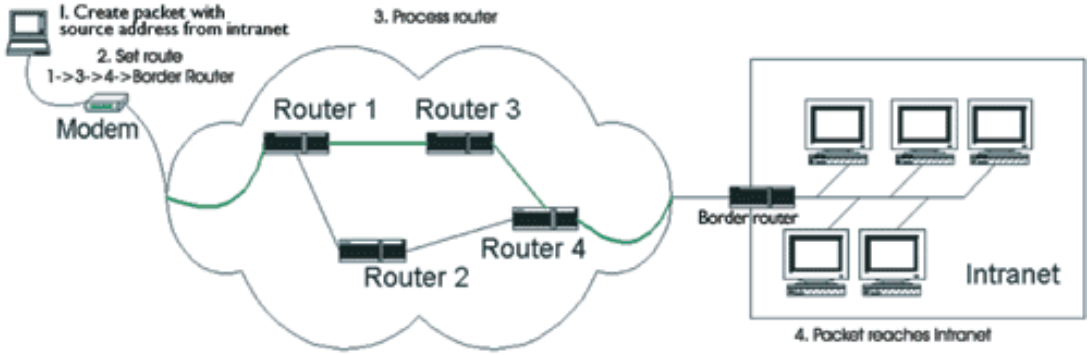



***Figura 2-20 Source Routing***

Otro problema son las redes amplificadas. Un paquete ICMP con una dirección fuente falsa será reenviado a una dirección broadcast en una red. Un router mal configurado permite el reenvío del paquete y la consecuencia es la respuesta de todos los huéspedes activos dentro del área local a la dirección fuente falsa. El huésped objetivo será inundado con paquetes y no podrá contestar al trafico normal (Denial of Service, DOS). Con un amplificador de red grande se puede interferir una conexión T1 (1.544 Mbps) con solo un modem a 14.4 Baudios. En este contexto es interesante que componentes de red mal configurados puedan causar este problema con solo un error.

Hay diferentes y muy populares formas de ataques DOS por ejemplo deshabilitando los servidores Web o FTP. Para potenciar la capacidad del DOS, los huéspedes en la Internet son infectados con Caballos de Troya que permiten ataques simultáneos desde varios hosts (Distributed Denial of Service). Especialmente están en peligro los dispositivos on-board desde que están equipados con menos recursos de memoria y potencia de cómputo. Algunas pruebas en laboratorio han mostrado que se puede incapacitar un bus acoplador con solo una PC causando una carga de CPU del 100% por envío de paquetes UDP.

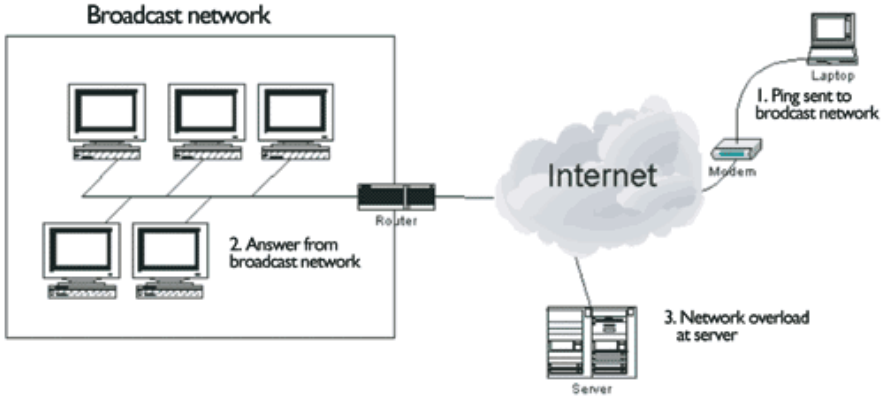



***Figura 2-21 Red Amplificada***

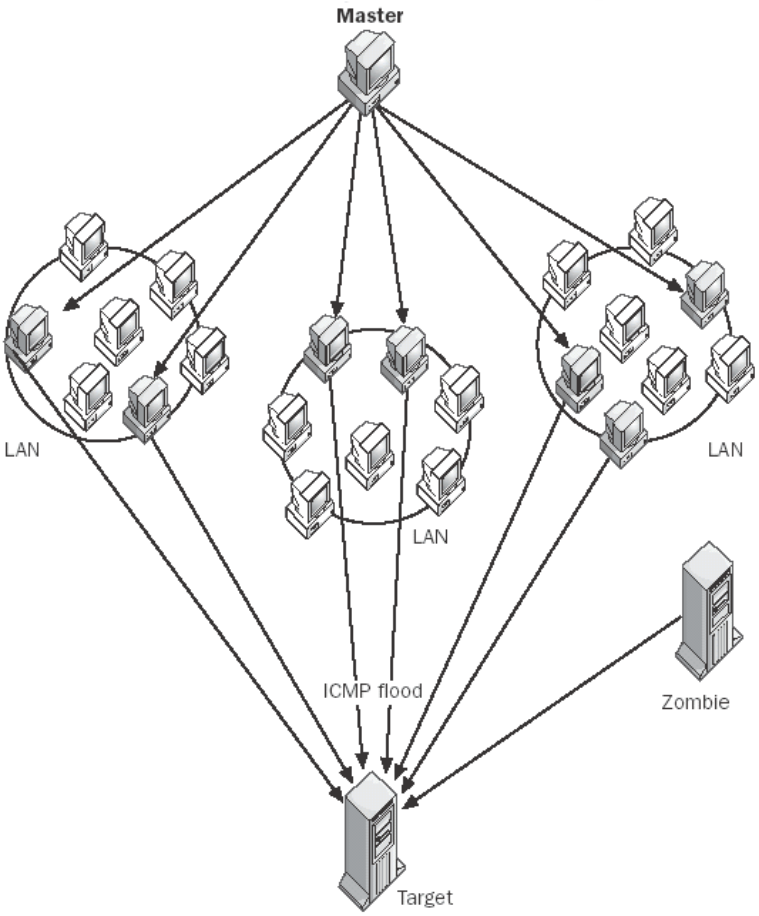



*Figura 2-22 Denial of Service Attack (DOS)*

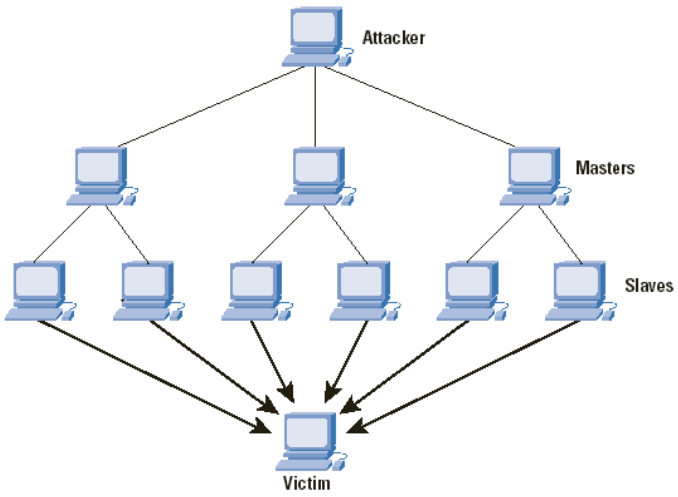



*Figura 2-23 Distributed Denial of Service Attack (DDOS)*

### 2.5.3 Implementación de flujos

Por supuesto los escenarios de ataque no están restringidos a los protocolos en si mismos. Muchos huecos de seguridad surgen con la programación. Por ejemplo unos muy populares son los Buffer Overflows (Sobre-flujo de Almacenamiento). Estos explotan el hecho que siempre rutinas de copiado de cadenas (string copy routines) no checan la longitud de la cadena a copiar y sobrescriben instrucciones de programa con cadenas especiales. Otros problemas pueden ser atribuidos a implementaciones de pila defectuosas. Por ejemplo hay problemas conocidos con los mecanismos MTU Discovery usados por los kernels modernos Linux. Con este método los sistemas operativos tratan de encontrar una trayectoria efectiva al objetivo fijando el Don't Fragment-Bit (Bit No-Fragmentado) en las cabeceras IP utilizadas. Este bit instruye al router para usar una conexión de red que puede transportar el paquete como un todo o enviar un mensaje de error ICMP de vuelta al emisor. Algunas pruebas han demostrado bloqueos de dispositivos on-board causados por este bit.

Basado en el conocimiento de los términos que el modelo "seguridad" y posibles flujos en la comunicación basada en Ethernet, IAONA JTWG Security ha definido una metodología paso a paso de cómo planear la seguridad para redes industriales Ethernet. Las siguientes secciones nos darán una breve introducción de esta metodología. Una descripción mas amplia y profunda a los tópicos de la seguridad pueden ser encontrados en el "IAONA Handbook Network Security".
Es importante notar que los siguientes pasos no necesitan ser secuenciales. En vez de eso, cada paso puede influenciar a otros pasos.

#### Paso 1: Clasificación por demanda de seguridad

A fin de definir que demanda de seguridad tiene un sistema sencillo, primero es necesario definir un grupo de categorías en las cuales un mal funcionamiento de un dispositivo puede tener efectos en:

- Afectación de la producción: Describe los efectos de una falla de un servicio o dispositivo en el entorno de producción.
- Seguridad del usuario (salud y vida): Describe como una falla puede afectar la seguridad del usuario.
- Afectación de la privacidad (acceso a datos relacionados a las personas): Describe como una falla guiar a una violación de la información relacionada a las personas.
- Afectación de la imagen de la compañía, publicidad: Describe como una falla puede causar daño a la imagen de la compañía.
- Pérdida financiera: Describe como pueden ser las pérdidas financieras debido a una falla.
- Violación de leyes/contratos: Describe como una falla puede guiar a una violación de los derechos de patentes o datos confidenciales.

Ahora cualquiera puede planear las categorías de arriba a cuatro niveles de seguridad yendo desde el nivel nulo, por el bajo-medio, alto y hasta el nivel muy alto. El IAONA Handbook Network Security proporciona una tabla donde cada categoría dada arriba, comportamiento aceptable en cada clase de seguridad se describe. Basado en este comportamiento, una clasificación de seguridad para cada dispositivo puede ser definida.

#### Paso 2: Relaciones de comunicación en una red empresarial

Cuando se establece la protección de una red es importante realizar que tipo de relaciones de comunicación existen en la compañía, entre lugares de la compañía y el mundo exterior y cuales de estas relaciones tienen que ser protegidas.

La *Figura 2-24* muestra dos sitios de la compañía (Intranet Company A & B) y varios puntos de acceso remoto de estos sitios de la compañía. La comunicación entre las compañías a los puntos de acceso remoto toma lugar vía la Internet.

La arquitectura común de redes de compañías más grandes consiste en diferentes Intranets que se comunican sobre la Internet. El termino Intranet describe en este contexto una red de área local (LAN) que ofrece la mayoría de servicios que son conocidos de la Internet como: Domain Name Service (DNS), E-Mail (SMTP, IMAP, POP3) o servidores web (HTTP, HTTPS) basado en la suite del protocolo IP. Dentro de la Intranet existen dos sub-redes lógicas: Oficina y Fábrica. Cada Intranet representa una rama de la compañía.

La red de oficina consiste mayormente de tecnología PC equipada con interfaces de red Ethernet usadas para llenar las tareas comunes de administración. Las aplicaciones más comunes en la fábrica dentro de esta área son las aplicaciones de oficina al nivel ERP. Los protocolos más utilizados basados en Ethernet son los usualmente conocidos protocolos Internet como Ethernet ordinario: TCP/IP, HTTP, FTP y otros.

La red de la fábrica representa las diferentes áreas de producción dentro de una sección y conecta las diferentes unidades de producción con sus dispositivos al sistema de control de la producción apropiado. Los datos transmitidos dentro de la red de la fabrica son producidos por diferentes niveles de aplicaciones de control yendo desde las típicas aplicaciones de Sistema de Ejecución de Manufactura (MES, Manufacturing Execution System) así como administración de ordenes o manejo de herramientas para aseguramiento de la calidad hasta aplicaciones de control en tiempo real dentro de una célula especial de manufactura. Las aplicaciones de mantenimiento y servicio son también usadas dentro de la red de la fábrica. Los protocolos usados dentro de la red de la fabrica son los mismos que en la red de oficina pero extendidos para protocolos industriales Ethernet especiales como son Ethernet/IP, Modbus/TCP, Ethernet Powerlink, EtherCat y SERCOS III, reflejando los diferentes requerimientos de tiempo real de los sistemas de control industrial.

En este contexto la Internet es tratada como una gran red de redes interconectadas definida por la Internet Engineering Task Force (IETF) en el comentario de petición (RFC, Request for Comment) 2026 como una colaboración internacional organizada de redes interconectadas, autónomas, las cuales soportan comunicación host-to-host a través de adhesión voluntaria a protocolos abiertos y procedimientos definidos por los estándares Internet.

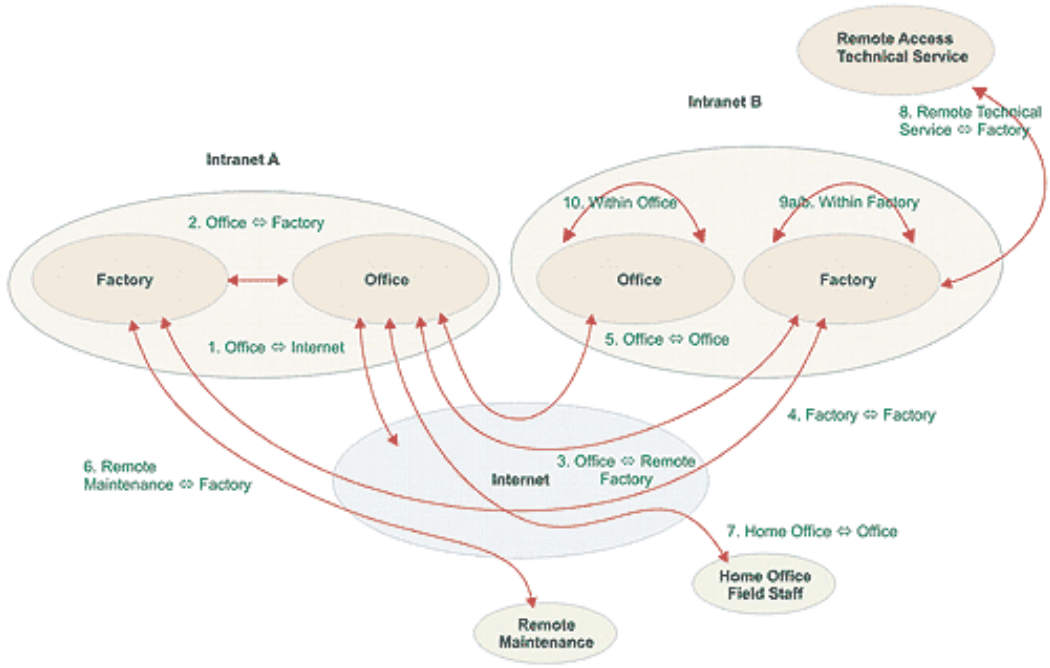



***Figura 2-24 Relaciones de comunicación con una red empresarial***

De acuerdo con la figura de arriba que muestra una red distribuida de una compañía las diferentes relaciones de comunicación se pueden describir como sigue:

1. Oficina ↔ Internet: Las PCs de oficina se comunican con la Internet para acceder a recursos de información que están localizados en esta red, por ejemplo accediendo a servidores web (HTTP) o bajando archivos (FTP). Esta comunicación no es de tiempo crítico y los paquetes de datos tienen un alto volumen.
2. Oficina ↔ Fabrica: ERP (Oficina) y MES (Fabrica) se comunican entre si para coordinar los procesos de manufactura. Esta comunicación es ligeramente de tiempo crítico y el volumen de los paquetes tienen un volumen medio.
3. Oficina ↔ Fabrica remota: ERP (Oficina) y MES (Fabrica remota) se comunican entre si para coordinar procesos de manufactura. Esta comunicación es ligeramente de tiempo crítico y el volumen de los paquetes tienen un volumen medio.
4. Fabrica ↔ Fabrica: Para coordinar procesos de producción entre distintas instalaciones, los MES de las instalaciones se deben comunicar entre si. Esta comunicación es ligeramente de tiempo crítico y el volumen de los paquetes tienen un volumen medio.
5. Oficina ↔ Oficina: La aplicación de oficina debe compartir datos entre secciones por ejemplo compartiendo documentos, coordinando manejo de procesos o intercambiando datos entre las partes de aplicación ERP. Esta comunicación no es de tiempo crítico y los paquetes de datos tienen un alto volumen.
6. Mantenimiento remoto ↔ Fábrica: Para mantenimiento remoto los fabricantes deben acceder a dispositivos dentro de la red de la fábrica. Esto puede ser hecho vía Internet, Intranet o desde la misma fabrica. Esta comunicación no es de tiempo crítico y los paquetes de datos tienen un volumen medio.
7. Oficina de casa / personal de campo ↔ Oficina: Los trabajadores de oficina en casa y miembros del personal de campo deben acceder y compartir sus datos dentro de la red de la oficina. Esta comunicación no es de tiempo crítico y los paquetes de datos tienen un alto volumen.
8. Acceso remoto del servicio técnico ↔ Fábrica: Un proveedor de servicio técnico puede acceder a la fábrica trayendo consigo una PC, un dispositivo o solo una unidad de almacenamiento. Esta comunicación no es de tiempo crítico y los paquetes de datos tienen un volumen medio.

9a. Dentro de la fábrica: Para coordinar el proceso de manufactura el sistema MES tiene que intercambiar datos con los dispositivos de control en campo dentro del sistema de control de piso en la fábrica. Esta comunicación ligeramente de tiempo critico y causa volumen de tráfico medio.

9b. Dentro de la fábrica: Para controlar el proceso de manufactura diferentes dispositivos del sistema de control intercambiaran datos. Esta comunicación es altamente de tiempo critico y causa volumen de trafico bajo.

10. Dentro de la oficina: Las aplicaciones de oficina deben compartir datos dentro de la red de oficina por ejemplo compartiendo documentos, coordinando administración de procesos o intercambiando datos entre las partes de aplicación ERP. Esta comunicación no es de tiempo crítico y causa un alto volumen de tráfico de red.

Basados en esta descripción genérica de relaciones de comunicación, el IAONA Handbook Network Security ofrece una plantilla para analizar dichas relaciones. Esta plantilla contiene las relaciones de comunicación (1-10) descritas arriba. Para cada relación, se puede especificar si las relaciones son:

- Necesarias
- Opcionales
- Prohibidas

Una amplia explicación de las posibles relaciones de comunicación así como una descripción detallada de la configuración estructural de una red de automatización se puede encontrar dentro del IAONA Handbook Network Security.

**Paso 3: Estrategia de defensa**

Basados en el resultado del paso 2, uno puede definir la estrategia de defensa. La estrategia de defensa define si uno quiere proteger la red en varios puntos formando diferentes zonas de seguridad (defensa profunda, defense-in-depth). Otra posibilidad es definir un muro impenetrable alrededor del sistema (perímetro rudo, hard-perimeter). La opción de la estrategia depende fuertemente del tipo de red.

**Paso 4: Estructuras de defensa**

Basados en las estrategias de defensa escogidas, ahora las estructuras de defensa necesitan ser especificadas. Esto significa como la defensa tomara lugar, por ejemplo, por medio de firewalls, ruteadores o switches y donde estarán posicionados en la arquitectura de comunicación.

Es importante notar que colocar se debe colocar la estructura de defensa en un nivel intermedio entre el nivel de seguridad y la funcionalidad. Como ya se indico en la primera sección de este subcapítulo de acuerdo con los términos relacionados a seguridad, podría no ser posible en todos los casos el llenar todos los criterios de seguridad los cuales pueden ser causados por varias razones. En áreas críticas de tiempo real la aplicación de filtros de paquetes es siempre difícil de realizar, mientras la aplicación de criptografía causa problemas en dispositivos on-chip debido a sus limitadas capacidades de procesamiento.

Una posibilidad de encontrar un remedio para este problema puede ser la estructuración de medidas de seguridad basadas en la estructura de red descrita en la *Figura 2-25*.

Como muestra la figura, el elemento básico de la red forma la célula de automatización. El tráfico de red dentro de esta célula tiene que ser procesado en tiempo real en la mayoría de los casos, por lo tanto la célula reacciona de forma muy sensitiva a influencias del exterior.
Mas adelante, tiene que prevenirse que software malicioso llamado “malware” se pueda dispersar entre diferentes células. Como una solución, un filtro de paquetes (el cual se puede integrar en un switch) puede ser usado y así conectar esa célula con la red de automatización.

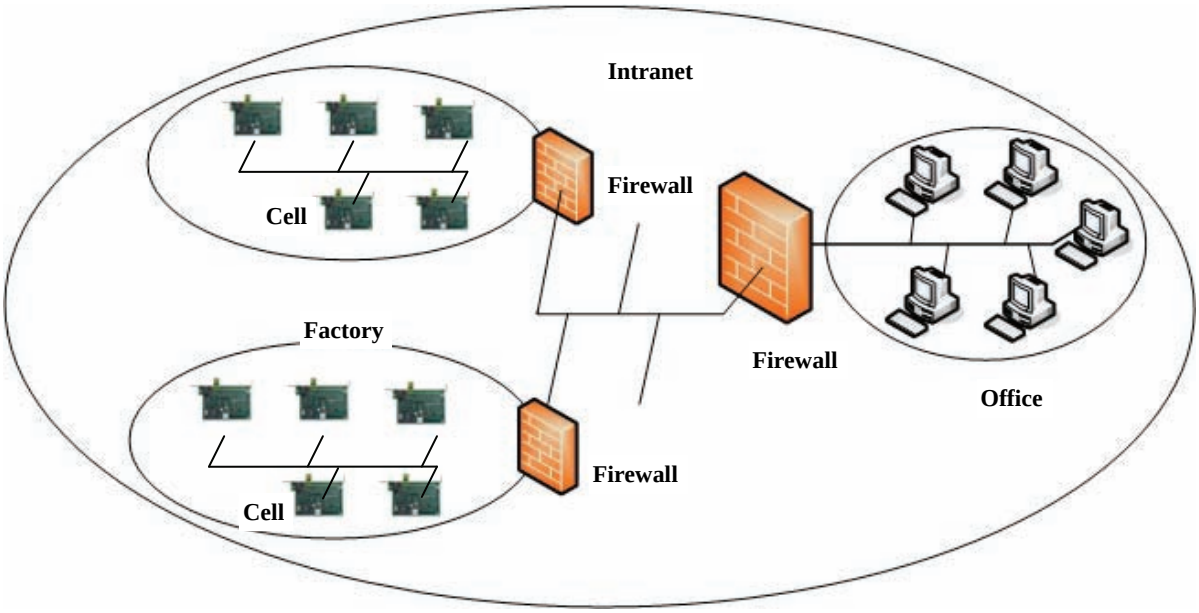



***Figura 2-25 Estructuración de medidas de seguridad***

Como ya se indico, el filtro de paquetes desempeña dos tareas esenciales:

- **Restricción de trafico entrante** para la célula: Esta medida principalmente actúa como una protección para las capacidades de tiempo real de la célula de automatización (por ejemplo: protección contra los Ataques por Denegación de Servicio). Como las situaciones no solo son causadas por acciones premeditadas, también pueden ser llevadas a cabo por uso indebido de utilerías de administración basadas en web o de igual manera por mala programación.
- **Restricción de propagación de malware** (por ejemplo virus o caballos de Troya): En caso de infiltración de malware en la célula de automatización (por ejemplo durante procesos de mantenimiento por personal externo para servicio en campo), la restricción de comunicación de red con otras células de automatización puede prevenir el malware para la propagación a través de la red y puede reducir el daño causado por este software.

**Paso 5: Dispositivos y protocolos**

Como siguiente paso, los dispositivos sencillos tienen que ser vistos con respecto a sus relaciones de comunicación y los protocolos los cuales son usados en estas relaciones de comunicación. Esto especialmente se refiere a los protocolos de automatización utilizados como Modbus/TCP, EtherNet/IP, Ethernet Powerlink o EtherCAT y sus puertos usados. La documentación de estos datos se requiere para definir las medidas de defensa y así definir las reglas del firewall a implementar.

Para hacer esto, la hoja de datos de seguridad IAONA (IAONA Security Data Sheet) puede ser de gran ayuda. Una SDS provee toda la información relacionada a seguridad como sistema operativo, mecanismos de respaldo así como una descripción de todos los servicios de red en un documento compacto.

La SDS IAONA puede ser aplicada para cualquier tipo de producto en el dominio de Ethernet Industrial, no esta limitada a un tipo especial de protocolo.

Esta podrá ser llenada y dada por junto con el producto por el proveedor de:

- Un dispositivo
- Células de producción o
- Un componente de infraestructura de red.

Basado en los datos de una SDS los consumidores pueden trabajar de forma segura con un producto. Todos los servicios de red en funcionamiento son documentados resolviendo el problema de tráfico de red desconocido. La lista de puertos/protocolos usados posibilitara al usuario para decidir como configurar sus firewalls / routers / switches.
En pocas palabras, los objetivos de una SDS son varios:

- Describir un producto
- Describir el comportamiento de la red
- Describir los puertos de red y servicios

El usuario o integrador del sistema colecta las diferentes SDS de los dispositivos en su sistema de automatización y deriva de estas SDS la información acerca de los diferentes protocolos que necesita para administrar su firewall. Las SDS están también disponibles en formato XML, de este modo las herramientas que pueden leer y procesar SDS pueden automatizar el proceso de la configuración de firewalls y otros componentes de seguridad. De esta forma, la complejidad de la aplicación de seguridad en una red Ethernet Industrial se reduce significativamente.
La IAONA esta proveyendo una herramienta para sus miembros con el fin de ayudarlos a llenar las SDS, se llama el SDS Creator IAONA (SDSC). Esta herramienta automáticamente genera archivos XML y PDF’s para imprimir. Una SDS sencilla puede ser salvada, cambiada, etc.

Después de compilar los conceptos para la infraestructura de la red de automatización, los protocolos usados tienen que ser considerados. Para este propósito, el "IAONA Handbook – Network Security" propone tanto una clasificación de seguridad para los protocolos (ranking security, clasificación de seguridad) y una recomendación de aplicación (rango de clasificación desde el 1=inseguro al 5=seguro). La clasificación de seguridad describe las características de los protocolos, por ejemplo, mecanismos de pérdida de seguridad, considerando que la clasificación provee indicaciones para la integración del protocolo (por ejemplo si el protocolo debería ser supervisado). Esta separación de la evaluación de un protocolo viene del hecho de que en algunos casos un protocolo inseguro es necesario para operar una red. Un punto de balance dentro del manual forma la descripción de 28 protocolos basados en Ethernet comunes en orden como se muestra en la *Tabla 2-5*.

Como una descripción contiene una pequeña explicación del protocolo, los puertos usados, una clasificación de seguridad y recomendaciones de aplicación con explicaciones adicionales. La descripción es completada por un ejemplo y medidas de seguridad recomendadas.

| | |
|---|---|
| Nombre | DHCP |
| Descripción | Dynamic Host Configuration Protocol |
| Numero de Puerto | 67, 68 |
| Rango de Seguridad | 2 (1=no seguro … 5=seguro) |
| Clasificación | 2 (1=no usar … 5=aconsejable) |
| Recomendación | Usar para redes cerradas o aplicaciones no criticas |
| Función | Dar configuración automática de huéspedes usando TCP/IP, abastece configuración IP, direcciona a servidores de nombres, routers, servidores de impresión, inicia imágenes para clientes sin disco y mucho mas |
| Uso | Principalmente usado para proveer parámetros de configuración a servidores Internet. Las maquinas clientes son provistas con sus direcciones IP así como con otros parámetros de configuración del huésped a través de este mecanismo. |
| Seguridad | La transferencia de datos es no cifrada |
| Peor Caso | Todos los huéspedes usando DHCP pueden no usar ninguna funcionalidad de red si el servidor DHCP esta averiado. |
| Medidas para seguridad | Usar configuración estática en vez de HDCP |

***Tabla 2-5 Descripción del Protocolo DHCP***

**Paso 6: Medidas de defensa**

El paso final cuando se aplica seguridad a una red es la aplicación de las medidas de defensa. Este paso se divide en dos partes principales:

- Configuración de los diferentes componentes de seguridad
- Definición de reglas organizacionales y administrativas

La configuración de diferentes componentes de seguridad esta basado en la definición de las relaciones de comunicación, la estrategia de defensa aplicada y la estructura, así como los dispositivos y protocolos dentro de la red. Este proceso se refiere especialmente a la configuración de firewalls a solo tráfico permitido que es marcado como necesario en la tabla de relaciones de comunicación (discutida en el paso 2). Pero el planear la seguridad de la red no termina con la configuración de esta. Además, esto es necesario para definir reglas administrativas como son la definición de protección de virus para todas las PC's conectadas a la red o reglas para incidentes como laptops robadas. Además se tienen que definir reglas para el servicio y mantenimiento que se da por medio de personal de servicio externo (como protección antivirus, parches, etc.).

## 2.6 Ethernet de tiempo real

Los sistemas de comunicación industrial deben ser capaces de satisfacer demandas muy estrictas, una pequeña falla de un sistema de comunicación puede ser la que encabece un mal funcionamiento del sistema completo y por esto las altas perdidas económicas en forma de bajas de producción o aun colisiones mecánicas y destrucción así como daños al personal.

### 2.6.1 Capacidad de tiempo real – ¿Que es el tiempo real?

Un importante requerimiento que muchas aplicaciones industriales demandan es la capacidad de tiempo real. Por principio se aclarara que comprende la capacidad de tiempo real y cuales diferentes capacidades de tiempo real pueden ser clasificadas en general.
Si un sistema es capaz de reaccionar bajo todas las condiciones de operación correctamente y dentro de las obligaciones de tiempo esperadas, entonces esta es la capacidad de tiempo real. Por consiguiente, si un sistema de comunicación satisface todos los requerimientos de tiempo para intercambio de datos de los componentes de cierta aplicación, esto es – relacionado a esta aplicación – la capacidad de tiempo real.
El determinismo es una palabra que esta muy ligada a la capacidad de tiempo real. El determinismo describe la predictibilidad exacta del comportamiento de tiempo en un sistema de comunicación.
Si es posible predecir exactamente el comportamiento temporal de un sistema en todos sus estados, entonces el sistema es estrictamente deterministico.

En principio las demandas de tiempo real pueden ser distinguidas en dos categorías.
La primera categoría simplemente requiere un tiempo máximo (deadline) hasta que una acción tiene que ser ejecutada y completada. Este es el requerimiento para el “timeliness”.
La segunda categoría requiere de un cierto tiempo especificado o time grid (reja de tiempo) en la cual una o varias acciones coordinadas tiene/tienen que ser completadas – en el ultimo caso es también una falla, cuando la acción es completada antes, este es el requerimiento para la sincronización. La desviación que puede ser tolerada se llama fluctuación (jitter). Formalmente – y por esto mas en general, las constantes de tiempo pueden ser presentadas para el uso de funciones de tiempo/utilidad.

Las funciones de tiempo/utilidad expresan la utilidad de ejecutar y completar una cierta acción como una función del punto de tiempo cuando la acción es ejecutada y completada. Los valores de utilidad expresan la relativa importancia de una acción.

De acuerdo con el modelo de función de Douglas Jensen de tiempo real, la primera categoría de timeliness implica que la utilidad de completar una acción es totalmente dada (valor 1) desde el tiempo cero hasta la deadline. La otra categoría de sincronización implica que la utilidad de ejecutar una acción es solo dada dentro de una pequeña ventana de tiempo alrededor de un tiempo de ejecución asignado (deadline). La ventana de tiempo esta determinada por la fluctuación aceptable de la deadline.

Para llevar a cabo la primera categoría (el requerimiento para timeliness), Ethernet Standard puede ser un protocolo apropiado para un amplio rango de aplicaciones. Con respecto a la segunda categoría, el requerimiento de sincronización puede no ser generalmente garantizado con Ethernet Standard. Esto es debido al hecho que una fluctuación no aceptable en la duración de la transmisión puede ser causada por retardos no predecibles en la cola del buffer de paquetes (packet buffer queues).

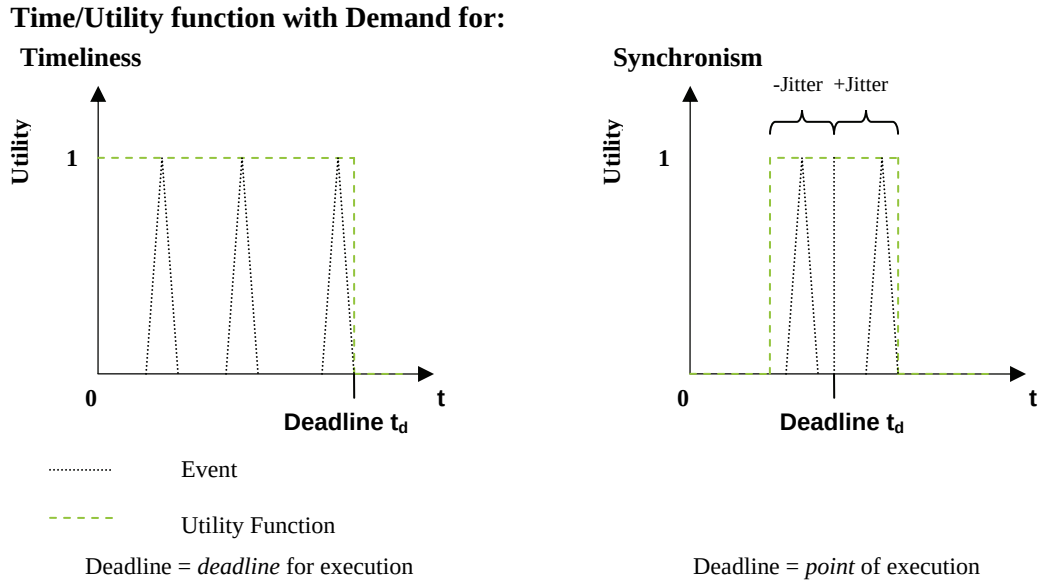



***Figura 2-26 Presentación general de funciones de Time/Utility de los requerimientos de Tiempo Real: Timeliness and Synchronism***

### 2.6.2 Desde sistemas fieldbus a comunicación de tiempo real basada en Ethernet

En automatización distribuida una coordinación precisa de diferentes secuencias de movimiento de actuadores es realizada por mecanismos de sincronización basados en tiempo. En tiempos antiguos esta comunicación entre actuadores, sensores y controles fue llenada completamente por fieldbuses especializados. Con esto, la ejecución de acciones esta completamente atada a los datos entrantes y al dispositivo de ejecución; esto significa, el patrón de tiempo de comunicación estrictamente determina el patrón de tiempo de ejecución.
Esa es la razón por la que el patrón de tiempo de comunicación fue realizado de una manera absolutamente deterministica que significa predecible.

En principio, Ethernet TCP/IP no es deterministico y originalmente fue creado para permitir múltiples computadoras con diferencias, desde cada una con diferentes trabajos para usar un solo medio de comunicación por igual. Esta es la razón por la cual las relaciones de comunicación dentro de la red son cambiadas constantemente y no siguen un patrón cíclico. De acuerdo a estas circunstancias la comunicación es organizada de forma flexible ya que el punto exacto de tiempo y duración de un intercambio de datos esta sujeto a bastantes y grandes variaciones.
Contra la integración vertical trasera de Ethernet – aun en el nivel de campo mas bajo – principalmente existen dos posibilidades para reaccionar: en primer lugar, es posible hacer el comportamiento de sistemas basados en Ethernet TCP/IP exactamente predecible – de otra manera no es posible asociar el “concepto de tiempo” de todo el sistema a las características del sistema de bus (conocidos como sistemas de fieldbus). En segundo lugar, esto puede ser necesario para diseñar soluciones totalmente nuevas para organizar la cooperación temporal precisa de ciclos en procesos de control.

Para la realización de la variante uno para algunos conceptos de control basados en Ethernet, existen conceptos de sincronización en el área de fieldbus por ejemplo el mecanismo de slot de tiempo de Powerlink, que fueron transferidos a PROFInet IRT o SERCOS III.
En EtherCAT un direccionamiento e intercambio de datos entre todos los participantes de la red es realizado vía un registro de cambio (shift register) el cual esta corriendo directamente a través de todos los dispositivos participantes.

Este enfoque para transferir mecanismos y conceptos para comunicación de fieldbus síncrona a Ethernet normalmente resulta en uno de los siguientes hechos:

- Ethernet TCP/IP no es o solo de forma muy limitada usado de acuerdo al estándar Ethernet original
- Solo Ethernet así como la capa 2 del protocolo como medio de transmisión rápida es usada

La universalidad requerida en comunicación, de este modo, es parcialmente limitada.
Otra posibilidad para mejorar la precisión temporal y sincronía de dispositivos de control basados en Ethernet – bajo perpetuación simultanea del estándar de conformidad Ethernet – ofrece la sincronización de relojes descentralizados. Esto posibilita el cumplimiento de control distribuido síncrono sin una organización síncrona de la respectiva comunicación; lo que significa una desconexión del patrón de tiempo de la ejecución de una aplicación desde el patrón de tiempo de su propia comunicación. Esta circunstancia se representa en la siguiente figura que describe un diagrama de tiempo/utilidad.

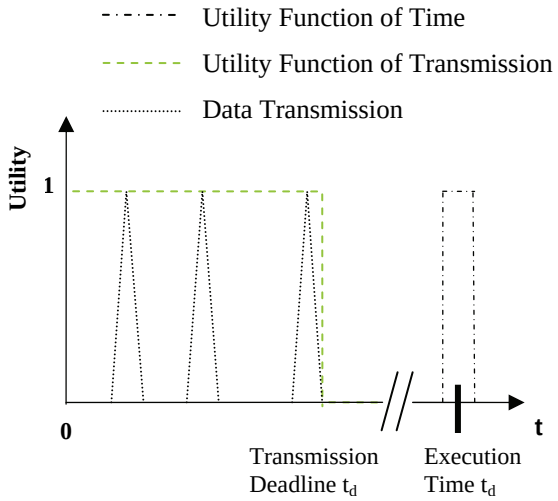



***Figura 2-27 Desconexión de la comunicación y Ejecución***

Las variaciones en el retardo de eventos en transmisiones de datos los cuales son típicamente para la tecnología Ethernet TCP/IP, son de este modo tolerables aun para la solución de sincronía, en trabajos de control altamente precisos. Esto tiene que ser visto como nuevo en tecnología de automatización desde las bases de comportamiento de tiempo real convencionales en determinismo absoluto todo esto sobre cadena completa de procesamiento de datos – incluyendo comunicación.
Un correspondiente tipo de algoritmos de sincronización los cuales pueden proveer una precisión de sincronización de alrededor de 1 microsegundo esta actualmente siendo desarrollado por el grupo de trabajo IEEE 1588.
La estructura de este artículo se subdivide en varias consideraciones para la adaptación estándar y el llenado completo de los requerimientos del timeliness industrial y además en consideraciones para el (no inherente) llenado completo de los requerimientos de sincronización industrial, considerando que especialmente el algoritmo de sincronización IEEE 1588 será direccionado.
La consideración de los requerimientos de timeliness incluyen la discusión de los pasos principales en el desarrollo de Ethernet en su camino de Ethernet clásico de oficina a un sistema de comunicación industrial aprobado.

### 2.6.3 Aspectos de red

Ethernet estuvo basado originalmente en CSMA/CD (Carrier Sense Multiple Access / Collision Detection). Un dispositivo terminal deseaba enviar datos y éste checa el medio de transmisión. Si la red no esta siendo usada por otro dispositivo, este comienza a transmitir. Como se ilustra en la figura de abajo es posible que varios dispositivos detecten que la red esta libre y simultáneamente empiecen a enviar datos.

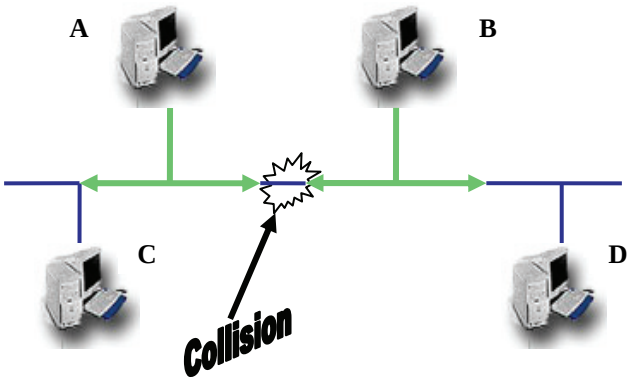



*Figura 2-28 Colisiones en Ethernet Clásico*

La colisión será detectada por los dispositivos terminales y todos ellos pararan la transmisión.
Estos intentaran de nuevo después de un periodo de tiempo aleatorio. De esta forma hay una alta probabilidad de que una colisión no ocurra de nuevo. Esta tecnología de acceso es intrínsecamente no deterministica, ya que el acceso a la red esta basado en probabilidad estadística. Este comportamiento ha resultado en la reputación de que Ethernet TCP, UDP/IP's es inadecuado para aplicaciones de tiempo real.

### 2.6.4 Switcheo

Las redes modernas basadas en Ethernet son mayormente construidas usando solo la tecnología de switcheo (distribución en estrella). En contraste a CSMA/CD aquí no se comparte el medio y en el cual los dispositivos terminales deben competir para acceder.
En vez de esto cada dispositivo terminal es asignado a una conexión full duplex al switch. Como resultado no hay contención para acceder al medio de transmisión y cada nodo de la red puede enviar datos de forma independientemente de las actividades de los otros nodos.

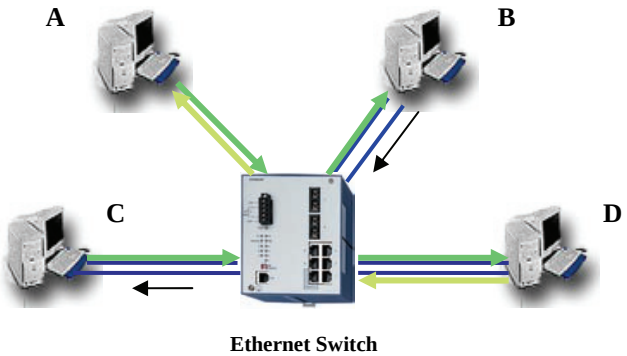



*Figura 2-29 Prevención de colisiones usando un Switch*

Es imposible que las colisiones ocurran. Los datos entrantes pueden ser inmediatamente switcheados a sus destinos. Por ejemplo, el dispositivo A puede enviar datos a B, mientras C simultáneamente envía datos a D, y D simultáneamente envía datos a A.

Complicaciones surgen si el dispositivo A envía datos a B y al mismo tiempo C también envía datos a B. En esta situación los datos serán almacenados (buffered) por el switch y transmitidos en secuencia. Esto es como las colas se desarrollan, incurriendo en retardos.
Si en una situación de la "vida real" el monto de los datos a ser transmitidos es claramente definido y el numero de dispositivos terminales es conocido, sujeto a la velocidad de transmisión de la red, el retardo máximo puede ser determinado. Indudablemente la fluctuación entre el retardo de tiempo mínimo y máximo no siempre es insignificante.

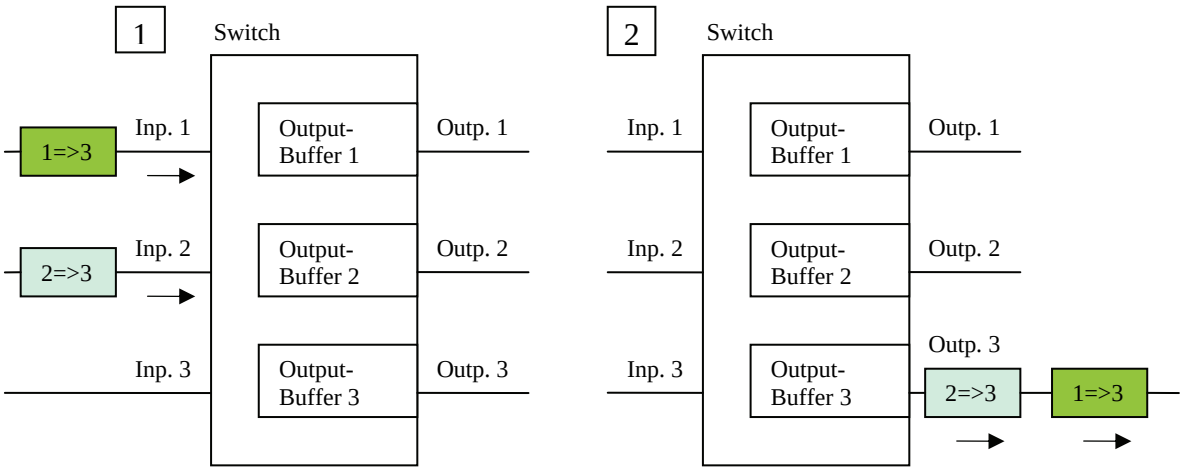



*Figura 2-30 Efecto de cola (Queuing Effect)*

### 2.6.5 Priorización de acuerdo al estándar IEEE 802.1p

Una importante mejora que Ethernet ofrece hace un par de años es el mecanismo de priorización en Capa 2, estandarizado por el grupo de trabajo 802.1p. Un campo adicional, conocido como tag (etiqueta), es sumado a la trama Ethernet. La etiqueta contiene información acerca de la prioridad de los datos.

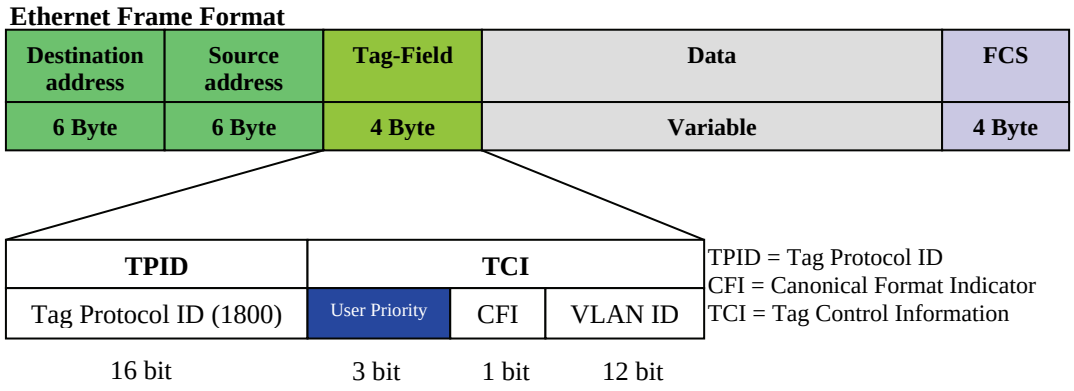



*Figura 2-31 Etiqueta de Prioridad de acuerdo a IEEE 802.1p*

Los switches usados dentro de una red de automatización deben soportar esta función. Pero no todos los productos soportan el amplio rango de niveles de prioridad y solo distinguen entre niveles de prioridad 2 o 4. Cada puerto de transmisión de un switch que soporta IEEE 802.1p tiene que separar la cola de cada nivel de prioridad soportado. Paquetes de datos de una alta prioridad en la cola son siempre transmitidos antes que aquellos de una baja prioridad en la cola.

### 2.6.6 Ethernet, Fast Ethernet y Gigabit Ethernet

Mientras que Ethernet fue originalmente diseñado con una tasa de transmisión de 10 MBit/s, desde 1995 este ha sido un estándar para 100 MBit/s (Fast Ethernet). En 1998 1000 MBit/s (Gigabit Ethernet) fue estandarizado y en el 2002 un estándar de 10 Gbit/s fue expedido. Hoy en día la mayoría de dispositivos terminales Ethernet soportan tanto tasas de transmisión de 10 MBit/s como de 100 MBit/s, Gigabit y 10Gigabit Ethernet ya se han establecido para uso en aplicaciones de backbones. El grupo IEEE 802.3 esta ahora discutiendo un estándar 100 Gigabit Ethernet.

Con cada aumento en la velocidad de trasmisión, el tiempo de transmisión para un paquete sencillo es reducido en un factor de 10. En una red a 10 Mbit/s le toma cerca de 1.2 ms transmitir el tamaño máximo de trama Ethernet de 1522 bytes. Usando Fast Ethernet este tiempo es de solo 120 µs, con Gigabit Ethernet solo 12 µs y con 10 Gigabit Ethernet solo 1.2 µs.

### 2.6.7 Comportamiento de tiempo real por segmentación

En adición al control de datos el cual requiere capacidad de comunicación en tiempo real, datos adicionales con diferentes perfiles de carga y características usaran la red. Por ejemplo, datos de visualización, actualizaciones de software, trafico de e-mail, aplicaciones de oficina y datos de trafico Internet.
Por esta razón la red debe estar meticulosamente diseñada, incluyendo la segmentación de aquellas partes de la red donde el comportamiento de tiempo real es necesario.

Los dispositivos terminales que requieren comportamiento de tiempo real deberán ser enlazados a los menos switches posibles. Inevitablemente, entre mas switches haya entre dos dispositivos terminales, la capacidad de procesamiento en “el peor caso” y el tiempo de cola se verán afectados significativamente. Con backbones y otras instancias donde no hay factores limitantes del rendimiento de tiempo real, los segmentos individuales son comúnmente conectados en estructura de anillo.

Sumado a esto, la interfaz entre un segmento de tiempo real y el resto de la red debe ser controlada de manera precisa. Ya que los datos de tráfico desde la red general pueden adoptar cualquier perfil cargado, esto debe monitorearse y restringirse cuando entran a un segmento de tiempo real.
Para prevenir que un segmento de tiempo real se sobrecargue, el monto del tráfico de datos entrantes a este segmento debe estar limitado. Una forma efectiva de conseguir esto es configurar el enlace entre segmentos a 10 Mbit/s, mientras todos los dispositivos en el segmento de tiempo real se comunican a 100 Mbit/s.

Además de la segmentación, un buen control de acceso puede ser logrado con el uso de routers y firewalls.

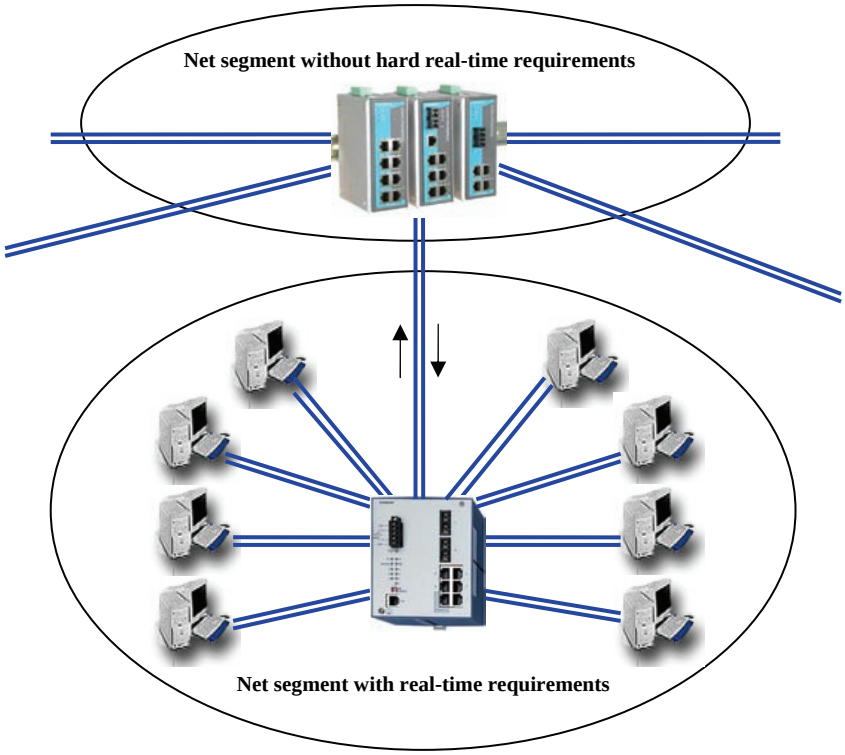



*Figura 2-32 Segmentación de red*

### 2.6.8 Problemas de transmisión de área (Problem Area Broadcast)

El número de tramas transmitidas en una red también es un factor que contribuye en la sobrecarga de la red. Por un lado la carga de transmisión de los dispositivos terminales, porque los dispositivos tienen que examinar cada transmisión. Por el otro lado dependiendo de la arquitectura de los switches, las transmisiones ponen carga adicional en estos. Esto es porque una trama broadcast tiene que ser duplicada por cada puerto de salida del switch. Para contrarrestar los efectos negativos del broadcast, algunos switches ofrecen una función conocida como “Broadcast Limiter”.
Esto limita a un umbral predefinido el número de transmisiones broadcast enviadas cada segundo.

### 2.6.9 Uso inteligente de la priorización

Una tercera posible vía en la cual el segmento de tiempo real puede ser alterado por el resto de la red es el uso inapropiado de tramas priorizadas. Normalmente la priorización dentro de células de tiempo real asegura que el trafico de datos cíclicos esta favorecido sobre el trafico de baja prioridad. Sin embargo, es posible que el trafico desde una célula exterior de tiempo real y también marcada con la misma alta prioridad sea transmitida en la célula.
Para prevenir esto, algunos switches soportan la habilidad de ajustar manualmente la prioridad del tráfico de datos para puertos específicos. Si el puerto del resto de la red es configurado con una prioridad baja, entonces el tráfico no puede interrumpir el tráfico de datos cíclicos.

### 2.6.10 TCP o UDP

TCP (Transmission Control Protocol), un protocolo de Capa 4 de la suite del protocolo Ethernet TCP, UDP/IP es un protocolo basado en conexión. Este establece una conexión virtual que comienza el proceso de comunicación, y cierra la conexión cuando el proceso de comunicación ha finalizado.

Como resultado, la perdida de datos puede ser detectada y ser retransmitida automáticamente. TCP también asegura que los restos de datos transmitidos se enviaran en la secuencia correcta.

En contraste a esto, UDP (User Datagram Protocol) es libre de conexión. Los paquetes de datos enviados son absolutamente independientes uno del otro. Para aplicaciones de tiempo real UDP es normalmente usado como protocolo de Capa 4, ya que la retransmisión y la capacidad de tiempo real son demandas contradictorias.
UDP es mas tolerante en la automatización industrial como en el caso de de una falla de transmisión simple con una completa perdida de datos para una actualización con los datos actuales en la siguiente transmisión. De manera opuesta, TCP podría repetir la transmisión con los datos no actualizados hasta que fuera exitoso el envío.

### 2.6.11 Cuellos de botella en la pila de los protocolos TCP, UDP/IP

En la mayoría de los casos los cuellos de botella en la transmisión de datos no son causados por la infraestructura de la red, pero si por las pilas de los protocolos las cuales son generalmente un componente del sistema operativo de tiempo real aplicado. Investigaciones de sistemas operativos típicos de tiempo real muestran que las pilas, como se usan hoy en día, tienen tiempos de procesamiento (throughput times) relativamente altas. Mediciones con sistemas Pentium a 400 MHz por ejemplo muestran tiempos alrededor de los 200 µs, con una fluctuación de menos de 10 µs.
Pruebas en otros sistemas muestran tiempos de procesamiento fluctuando alrededor de cinco veces este nivel.

Consecuentemente índices reducidos concernientes al comportamiento de tiempo pueden ser asumidos. Claro que con CPU's mas potentes y menor tiempo de respuesta del CPU, los tiempos de proceso son menores. En casos específicos una declaración acerca del comportamiento de tiempo de funcionamiento de la pila deberá ser solicitada desde el proveedor al sistema operativo que esta siendo utilizado.

Mientras tanto ahí están los proveedores del sistema operativo y pila de red, quienes han mejorado sus productos concernientes al tiempo de funcionamiento de la red. Si las pila del protocolo se realizan en hardware, el software de protocolo de red es completamente removido desde la CPU. Este es manejado en un chip separado, el cual se localiza entre los chips CPU y Ethernet. De esta forma el tiempo de procesamiento de la Capa 3 y 4 es claramente mejorado comparado con cualquier implementación de software y llega a ser completamente independiente de todas las demás operaciones.

Desde la perspectiva de red, mas mejoramiento se puede conseguir si los dispositivos terminales se comunican usando Gigabit Ethernet. Aun si hoy en día el precio de Gigabit Ethernet confina su uso a los backbones o posiblemente grandes sistemas de servidores, el progreso en la tecnología de semiconductores reducirá dramáticamente los costos dentro de unos pocos años. Esto muestra claramente como la automatización se beneficia automáticamente en el presente y en el futuro del desarrollo internacional de Ethernet como un estándar de comunicación abierto.
En suma, características como la priorización, tasa de limitación (de datos), y preparado de tasa (rate shaping) que es un suavizado del perfil leído (smooth of the load profile), se encontraran con mayor aceptación y difusión.

### 2.6.12 Arquitecturas genéricas de los protocolos de automatización basados en Ethernet

A partir de las consideraciones de la figura siguiente en principio tres variantes de arquitectura genéricas para capacidad de tiempo real en los protocolos de comunicación basados en Ethernet pueden ser derivadas.

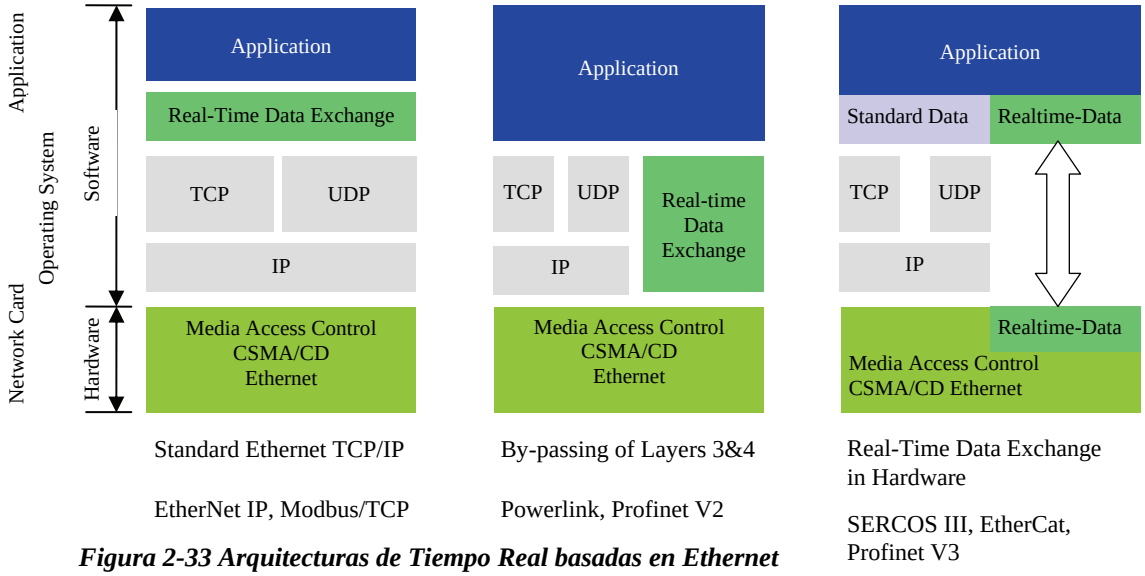



***Figura 2-33 Arquitecturas de Tiempo Real basadas en Ethernet***

En la arquitectura presentada del lado izquierdo de la figura el intercambio de datos de tiempo no crítico y el intercambio de datos de tiempo real son llevados sobre la pila estándar TCP/UDP/IP. La arquitectura que está a la mitad de la figura y la de la derecha realizan un bypass (desviación) de la pila TCP/UDP/IP para el intercambio de datos de tiempo real. Considerando que la realización del intercambio de datos de tiempo real puede ser distinguido entre implementaciones de software y hardware.

El tiempo hasta que los datos de usuario pueden ser realmente procesados en la aplicación o convertidos físicamente, también depende adicionalmente de la estructura organizacional respectiva (por ejemplo el modelo objeto) del protocolo de automatización simple. Además factores de influencia que dependen del respectivo protocolo de automatización son por ejemplo la topología de red física y lógica, la habilidad multicast y broadcast – como una posibilidad para enviar el mismo datagrama al mismo tiempo a múltiples receptores – o el tipo de intercambio de datos: mensaje orientado o método de suma de tramas así como el sistema jerárquico subyacente.

### 2.6.13 Clases de tiempo real IAONA

Para facilitar la decisión del proceso de preparación de los usuarios finales concernientes a los dispositivos apropiados y sistemas para sus aplicaciones, el IAONA Joint Technical Working Group Hard Real-Time hizo una propuesta para etiquetar las capacidades de tiempo real. Las bases de sistematización en los tres factores principales: latencia, sincronización y ancho de banda.
Con la ayuda de la sistematización los requerimientos de una aplicación y también el rendimiento de dispositivos pueden ser etiquetados y fácilmente comparados o afinados con algún otro.

| Sistematización en relación a Sincronismo, Latencia y Ancho de Banda<br>Clasificación de Tiempo Real IAONA IRC – X – Y – Z (IAONA Real-time Classification) | | | | | |
|---|---|---|---|---|---|
| Considerando para Latencia (X): | | Considerando para Sincronismo (Y): | | Considerando para Ancho de Banda (Z): | |
| No requerimientos | X | No requerimientos | X | | |
| > 100 ms | A | > 100 ms | A | > 10 MBit/s | A / + Design, in byte |
| 30 ms – 100 ms | B | 1 ms – 10 ms | B | 10 MBit/s – 100 MBit/s | B |
| 10 ms – 30 ms | C | 100 µs – 1 ms | C | 100 Mbit/s – 1 Gbit/s | C |
| 3 ms – 10 ms | D | 10 µs – 100 µs | D | 1 Gbit/s – 10 Gbit/s | D |
| 1 ms – 10 ms | E | 1 µs – 10 µs | E | | |
| 300 µs – 1 ms | F | | | | |

***Tabla 2-6 Clasificación IAONA de Tiempo Real***

### 2.6.14 Sincronización por relojes de tiempo real distribuidos – IEEE 1588

Como se había mencionado anteriormente, usando relojes de tiempo real distribuidos una desconexión de la red de tiempo de ejecución de la aplicación y de la red de tiempo de ejecución de la comunicación puede ser alcanzada. Debido a la importancia del estándar IEEE 1588 este se considerará de manera más amplia. Esta importancia del IEEE 1588 viene debido a su simplicidad y escalabilidad, la exactitud conseguida tanto como el desarrollo especifico para tareas de automatización – el estándar típico – de libre disponibilidad.
Protocolos de sincronización del mundo IT como NTP rsp o SNTP no pueden llenar los requerimientos especiales para automatización. Muchos proveedores de sistemas de control también con diferentes grupos como objetivo ya han implementado la tecnología especificada en este estándar en sus sistemas y productos. Los productos, aun si están basados en implementaciones propietarias, como los existente JetSync de la compañía Setter han implementado ya este estándar. Powerlink (de EPSG) y EtherCat (de ETG) serán extendidos con el estándar IEEE 1588 también.
La ODVA esta en el proceso de integrar el protocolo a EtherNet/IP bajo los nombres CIP Sync y CIP Motion. Con implementaciones ajustando el estándar, también sistemas de diferentes fabricantes pueden ser sincronizados entre cada uno sin problemas.

El estándar IEEE 1588 especifica un protocolo para una sincronización de reloj precisa para sistemas de control y medición. Este protocolo abierto es llamado de forma corta PTP (Precision Time Protocol), este conviene muy bien para la implementación en Ethernet TCP/IP y posibilita la realización de tareas de sincronización altamente precisas hasta el subrango de microsegundos y provee al mismo tiempo la transparencia vertical demandad por el uso de las pilas estándar Ethernet TCP/UDP/IP. La exactitud alcanzada principalmente depende del tipo de implementación. Requerimientos típicos de la automatización como alta precisión, esfuerzos de administración mínimos y optimización para componentes estables en un entorno seguro de conexión con un mínimo uso de recursos (procesador, red) están totalmente cubiertos.

#### 2.6.14.1 El principio básico

El principio básico de la sincronización de acuerdo al estándar IEEE 1588 consiste en grabar el tiempo de envío y el tiempo de recepción de paquetes especiales entre relojes (en tiempo real) locales y en la transmisión de estos valores en datagramas sellados de tiempo y del tipo especial. De acuerdo a esta grabación de tiempo, la desviación de los relojes y el retardo de transmisión en la red pueden ser calculados. Por el uso de relojes locales cada nodo en la red dispone del tiempo de sistema de forma totalmente precisa. Esto provee la independencia de la exactitud del tiempo de ejecución y de los comandos de control sincronizados de posibles desviaciones en la red de comunicación.
Esto hace a esta técnica especialmente interesante por el uso en sistemas basados en Ethernet, ya que esto permite a Ethernet TCP/IP – sin cambios básicos – ser usado para las redes dentro de sistemas de control altamente precisos. La exactitud conseguida excede a aquellos sistemas basados en fieldbus.

#### 2.6.14.2 Componentes del sistema

Los sistemas 1588 y PTP consisten en varios nodos, todos representando un reloj. Los relojes son conectados con cada uno vía una red. En principio hay dos tipos de reloj: relojes ordinarios y relojes de límite o frontera. La diferencia entre ellos es que un reloj ordinario tiene un puerto PTP sencillo y un reloj de límite tiene más de un puerto PTP sencillo. Desde el punto de vista de la red un reloj puede tener uno de los estatus generales: reloj esclavo, reloj maestro o gran reloj maestro.

Un sistema simple consiste en relojes esclavos y un reloj maestro. Si hay varios relojes maestros potenciales el reloj maestro activo será determinado de acuerdo a un algoritmo para encontrar al mejor reloj.

Todos los relojes esclavos permanentemente comparan sus caracterizaciones de reloj con la del reloj maestro actual, si hay por ejemplo nuevos relojes sumados al sistema o el reloj maestro actual es repentinamente desconectado, entonces los otros relojes realizan el algoritmo y un nuevo maestro se determinara por si solo.

Si varios subsistemas PTP necesitan ser conectados con algún otro, la conexión deberá exclusivamente ser realizada por un reloj de límite. Exactamente un puerto del reloj de límite trabaja como puerto esclavo, este puerto es conectado al subsistema que provee el tiempo para todo el sistema. Por lo tanto el reloj maestro de este subsistema es el gran reloj maestro para todo el sistema. Los otros puertos del reloj de límite trabajan como puertos maestros, sobre estos puertos del reloj de límite los mensajes para la sincronización de los subsistemas serán enviados. El puerto del reloj de límite aparece conectado al subsistema como si este fuera un reloj ordinario.

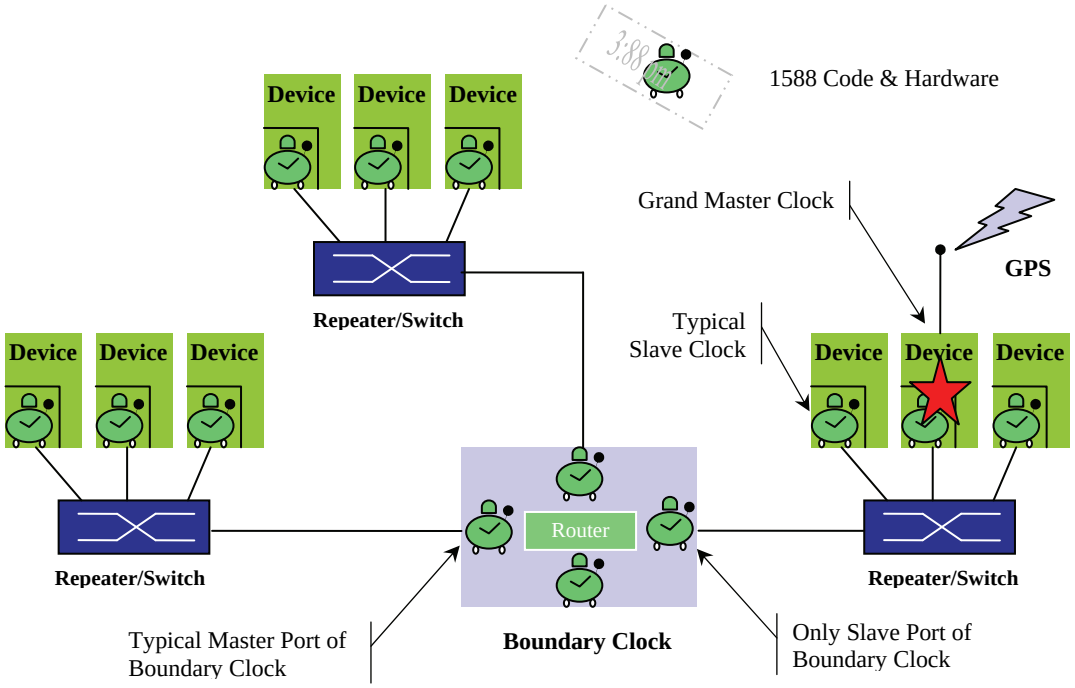



***Figura 2-34 Sistema IEEE 1588***

### 2.6.14.3 Mensajes de tiempo específicos

Además del manejo de mensajes, el protocolo PTP define cuatro tipos de mensajes que son enviados por envío multicast: un mensaje de sincronización, brevemente llamado Sync, un mensaje seguido del Sync, llamado brevemente Follow_Up, un mensaje de petición de retardo, llamado Delay_Req y una respuesta al Delay_Req, llamado Delay_Resp.
La reacción de un reloj en la recepción de un mensaje depende del estado actual del reloj. El mensaje Sync será enviado periódicamente (típicamente cada 2 segundos) desde el reloj que esta en el estado de reloj maestro. Éste también contiene las características de reloj del transmisor que son necesarias para el algoritmo de mejor maestro.

Primero que todo, el mensaje Sync contiene un sello de tiempo (timestamp), la cual – tan precisa como es posible – especifica el tiempo de envío estimado de ese paquete. Desde el tiempo de envío estimado tiene que ser integrado en el paquete antes de que se envíe realmente, el tiempo de envío real puede diferir del estimado. Porque ese, el tiempo de envío preciso de un mensaje Sync es medido y enviado en un mensaje siguiente Follow_Up. El receptor de un mensaje Sync graba su tiempo de recepción preciso.

Usando el tiempo de envío preciso contenido en el mensaje Follow_Up y el tiempo preciso de recepción, la desviación del reloj esclavo desde el reloj maestro puede ser calculada y el tiempo de esclavo puede ser por consiguiente corregido.

Sin embargo, la desviación determinada sigue incluyendo el retardo de la transmisión de la red. Para determinar este retraso de transmisión el mensaje Delay_Req es utilizado. Un Delay_Req será enviado desde un reloj esclavo después de la recepción de un mensaje Sync. Equivalente a un mensaje Sync el transmisor graba el tiempo de envío preciso y el reloj maestro como destinatario graba el tiempo preciso de recepción. El tiempo de recepción preciso es enviado dentro de un mensaje Delay_Resp, donde el retraso de transmisión acordado puede ser calculado y considerado para el siguiente calculo de la desviación del reloj.

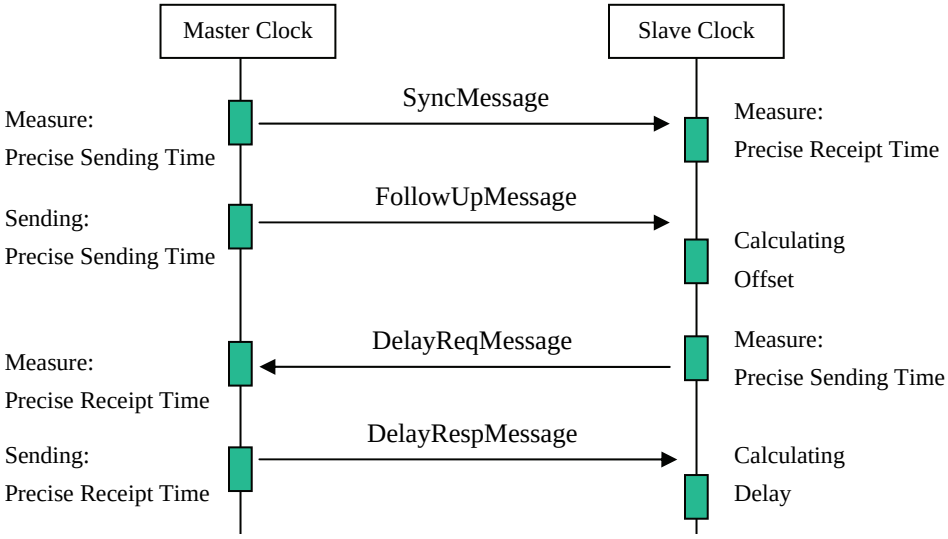



***Figura 2-35 Mensajes de tiempo IEEE 1588***

### 2.6.14.4 Aspectos de implementación

La precisión de la sincronización – la fluctuación de sincronización – depende fuertemente del tipo de realización de la implementación del sello de tiempo (time stamp implementation) y la detección de los mensajes de tiempo.

En el estándar IEEE 1588 estrictamente hablado, la generación de los correspondientes sellos de tiempo pueden ser implementados en diferentes niveles del modelo de 7 capas ISO/OSI. Esto resulta en exactitudes variables de la sincronización de los relojes. La realización de las Capas 1 y 2 del modelo ISO/OSI sucede en el hardware. En consecuencia, el retardo generado aquí esta sujeto a solo pequeñas variaciones las cuales hacen una implementación óptima del sello de tiempo aquí, pero debido a la acción del hardware también más compleja. Las variaciones que emergen aquí son en primera instancia dependientes del modo de operación de los componentes de infraestructura de la red activa. La Capa 3 es la primera capa realizada en software y normalmente es parte del sistema operativo, en consecuencia, entre las Capas 2 y 3 mayormente la transición de hardware a software toma lugar. La posibilidad de realizar un sello de tiempo en software, pero tan cercano como es posible al hardware se da aquí.

Una implementación en las Capas 4 a 6 obviamente podría causar los mismos esfuerzos, pero podrían ser de menor valor y, de este modo no serán vistas ni consideradas mas.
Una implementación en la Capa de Aplicación es posible sin ninguna interacción con el sistema operativo – y de este modo la forma mas fácil para la implementación IEEE 1588, indudablemente por el procesamiento técnico (por software) dentro de las capas subyacentes y durante la transición entre las capas sencillas relativamente variaciones fuertes con respecto al retardo total son dadas.

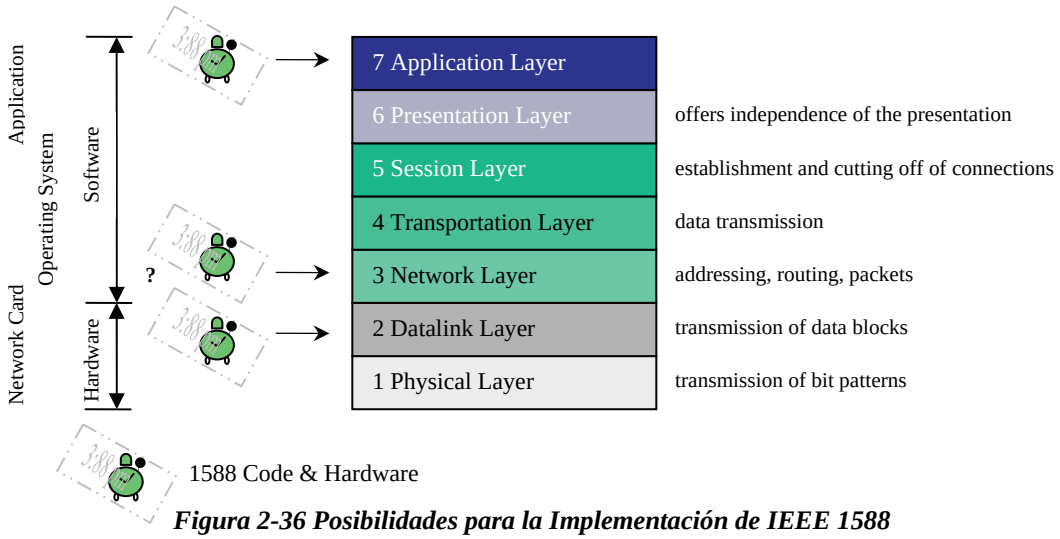



***Figura 2-36 Posibilidades para la Implementación de IEEE 1588***

El estándar recomienda para implementar el sello de tiempo tan cercano como sea posible a la capa física para evitar retardos variables dentro de la pila de comunicación. Implementaciones del sello de tiempo en la capa de aplicación resultan en exactitudes de 100 µs a 10 ms. El rango exacto depende del sistema operativo respectivo.

| Nivel de Implementación | Exactitud alcanzable |
|---|---|
| Nivel de Aplicación | 100 µs to 10 ms |
| Nivel de Interrupción | 10 µs |
| Hardware, Capa física | 500 – 50 ns |

***Tabla 2-7 Exactitud de la Sincronización dependiente del Nivel de Implementación***

Implementaciones del sello de tiempo en la Capa de Red resultan en variaciones típicas alrededor de los 10 µs. Una exactitud dentro del rango de los nanosegundos se puede conseguir y significa una implementación del sello de tiempo en hardware directamente sobre la Capa Física. Aquí, las variaciones pueden ser adicionalmente reducidas por medio de un diseño razonable del algoritmo de los relojes para ajuste de tiempo.

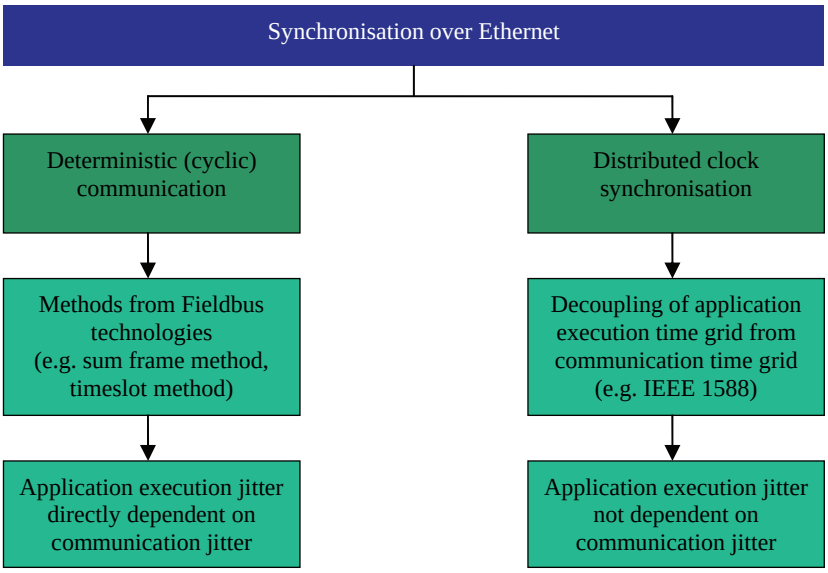



***Figura 2-37 Métodos de Sincronización sobre Ethernet***

## 2.7 Wireless LAN

Hoy en día, la tecnología Wireless LAN (LAN sin cables) es siempre utilizada para establecer una conexión inalámbrica a redes corporativas basadas en IP. Con el incremento de la aplicación de la tecnología Ethernet en las fábricas también las WLAN (Wide Local Area Network) están incrementando su popularidad en la industria. Siguiendo a los dispositivos de campo funcionando con redes Ethernet ahora la integración de dispositivos de control de campo dentro de sistemas WLAN esta emergiendo. Por consecuencia, esto puede ser posible de realizar para aplicaciones de tiempo real usando soluciones WLAN.

### 2.7.1 Términos básicos acerca de WLAN

La tecnología de red de radiocomunicación esta basada en el estándar IEEE 802.11 y es conocido básicamente como Wireless LAN. Esta tecnología habilita a una red wireless basada en IP dando al usuario la sensación de ser una red Ethernet TCP/IP ordinaria basada en un set de protocolos y tecnologías que utilizan ondas de radio como medio de comunicación físico. WLAN fue estandarizado desde 1999 y cubre con un par de sub-estándares un amplio rango de frecuencias de radio comunicación y tasas de transmisión de datos.

La estructura básica de un sistema WLAN esta dado por una estación WLAN básica llamada Access Point (Punto de Acceso) o algunas veces conocida también como Gateway, conectado a una red Ethernet ordinaria suministrando una célula de radio. Dentro de esta célula los clientes pueden acceder a la radio comunicación llegando a integrarse a la red Ethernet usando la radiocomunicación como punto de acceso inalámbrico a la red Ethernet.
Ya que los Access Points pueden adicionalmente trabajar como clientes WLAN, una red de varios access points es capaz de funcionar como una red inalámbrica.
La comunicación utilizando la familia de estándares IEEE 802.11 difiere con respecto a las frecuencias y tasas de transmisión de datos, estando desde los 2.4 GHz con 1.2 MBit dentro del estándar básico IEEE 802.11 hasta los 2.4 GHz y 54 MBit dentro del estándar IEEE 802.11g y 5 GHz y 54 MBit dentro del estándar IEEE 802.11a hasta los 5 GHz y 500 MBit dentro del próximo estándar IEEE 802.11n.

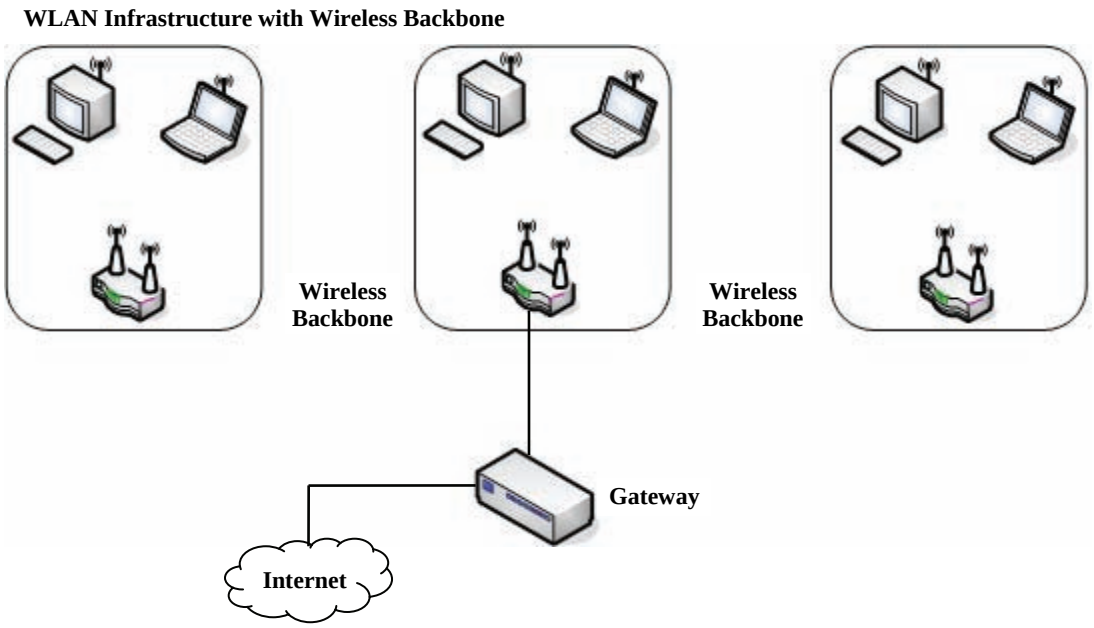



*Figura 2-38 Estructura básica de un nivel de trabajo WLAN*

Pero con el incremento de la frecuencia y la tasa de transmisión la dimensión de la célula de ondas de radio y por lo tanto la distancia máxima entre el access point y el cliente decrece. De manera clara la distancia máxima posible entre el access point y el cliente depende de los materiales entre ellos y los alrededores dentro del sistema WLAN utilizado. Como se sabe, el ferroconcreto así como muchos transmisores de interferencia vienen de sistemas de consumo de energía eléctrica y reducen la distancia máxima significativamente. Adicionalmente, la propagación de ondas de radio es comparable a la propagación de reflexiones de luz, interfiere con sus propias ondas y este efecto es aplicable también a los sistemas WLAN. Por lo tanto, en el campo abierto la distancia máxima entre un access point y un cliente es de 300 metros. Dentro del área de oficina esto se puede asumir a 50 metros. En las fábricas puede ser menor de 50 metros.
Antenas especiales en la estación WLAN y en el cliente pueden extender la distancia máxima significativamente. Distancias de hasta 20 kilómetros es posible conseguir con estas antenas.

Para reducir la influencia de frecuencias parasitas en la calidad de la transmisión y de este modo posibilitar una capacidad de procesamiento máximo del sistema WLAN, se pueden aplicar estrategias especiales. Estas se conocen como FHSS (Frequency Hopping Spread Spectrum) y DSSS (Direct Sequence Spread Spectrum).
Ambas tecnologías aplican la banda de onda completa del sistema WLAN. En el caso de los 2.4 GHz esta banda tiene un ancho de banda de 83 MHz la cual esta disponible para transmisión de datos. Dentro de esta banda diferentes frecuencias pueden ser utilizadas.

FHSS usa las diferentes sub-frecuencias en una secuencia predefinida. Ambos, el access point y el cliente conocen la secuencia de sub-frecuencias utilizadas. Si una sub-frecuencia es perturbada la transmisión será repetida en otra sub-frecuencia. DSSS aplica todas las sub-secuencias simultáneamente. Los bits transmitidos serán codificados de una forma pseudo-aleatoria e impresa en todas las sub-frecuencias. Ambos, el access point y el cliente saben la forma de codificar así que el receptor de una transmisión es capaz de decodificar el mensaje. Ambas estrategias, FHSS y DSSS evitan la influencia de frecuencias parasitas con un pequeño ancho de banda.
Pero estas no pueden evitar problemas resultantes de una sobrecarga de la frecuencia WLAN la cual puede ocurrir si más sistemas corren en paralelo.

### 2.7.2 WLAN en la industria: Incrementando la flexibilidad, disminuyendo costos

Usando la tecnología WLAN en aplicaciones industriales ofrece no solo considerablemente más flexibilidad. También les puede ahorrar a compañías y organizaciones un significante monto de dinero. Dentro de los sistemas de control distribuido modernos los sensores y actuadores están más y mas equipados con inteligencia y actualmente se les llama “controles inteligentes”, los cuales entregan más calidad de control que los dispositivos convencionales. Estos sistemas tienen que ser conectados a un PLC superior donde los datos necesarios están más y más basados en la comunicación Ethernet e IP.

La mayor parte de los costos que involucran a un sistema de control de esta naturaleza se pueden atribuir al cableado – en este caso el cableado Ethernet. Si los cambios y adaptaciones llegaran a ser necesarias durante el desarrollo o la aplicación del sistema de control, esto se traduce en altos costos de conexión adicionales para la conexión de sensores o actuadores extra o al menos el reemplazo del sistema de cableado. Aquí la aplicación de los sistemas WLAN puede reducir los costos e incrementar la flexibilidad del sistema con respecto a las adaptaciones necesarias para el sistema. Esto se puede ver en el siguiente escenario de aplicación.

Primero que todo, un Access Point esta conectado al puerto Ethernet de una unidad de control superior para cada maquina individual o robot de control. Entonces cada integrante puede ser implementado de forma inalámbrica en la célula de radio extendida por el access point.

Los clientes inalámbricos están equipados con una interfaz Ethernet para conectar los sensores y actuadores; nuevos desarrollos ya integran módulos de radio WLAN directamente en controladores inteligentes, lo cual significa que el cambio de elementos puede ser de forma mas rápida, y la implementación de sensores adicionales no presenta problemas tampoco.

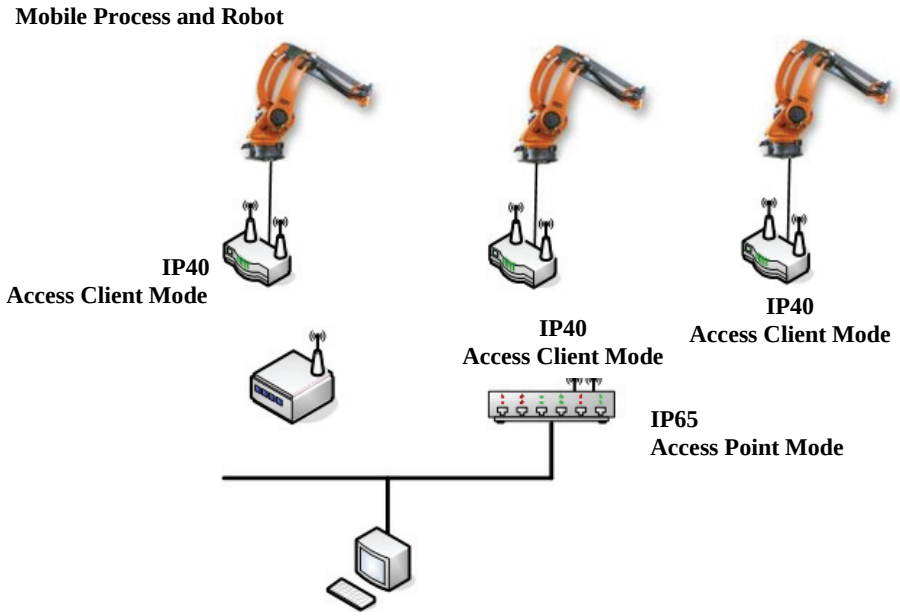



*Figura 2-39 Aplicación de las redes WLAN en automatización industrial*

La mayor ventaja, sin embargo, es el acceso directo a los sensores en el nivel IP. Los controladores inteligentes están también equipados con servidor Web integrado para propósitos de parametrización, con lo cual una solución WLAN también puede utilizarse para obtener acceso inalámbrico a los sensores. Esto hace posible transmitir el estado actual y datos de diagnostico durante la operación fuera de la zona peligrosa de la maquinaria a ser evaluada en una laptop. Los adaptadores WLAN ya son construidos en equipo de mantenimiento y diagnostico en el sector automotriz así que el último software y firmware puede ser mantenido en el equipo desde la oficina vía Internet.

### 2.7.3 Manufactura integrada a la computadora

Desde que la tecnología de la computadora ha encontrando su camino en los procesos de producción a un limite aun en crecimiento, las estaciones de procesamiento de red con las correspondientes computadoras son ahora indispensables. En este caso, una red inalámbrica ofrece las mas diversas opciones para el enlace de PC's con algunas otras. Utilizando terminales móviles o PDA's, es ahora posible algún flujo de material directamente. En suma, todos los pasos de producción pueden ser monitoreados en cualquier punto y a cualquier hora durante los procesos de producción y cualquier falla que pudiera ocurrir puede ser eliminada por consiguiente.
La supervisión completa de cada paso en el proceso de producción optimiza el control de calidad del producto, lo que se traduce en ahorro de costos.

### 2.7.4 Access Points que satisfacen las necesidades industriales

El prerrequisito para estas aplicaciones son access points que cumplan las necesidades industriales. Los dispositivos son requeridos para corresponder con todos los estándares IP populares, incluyendo aquellos en los que dominan las condiciones ambientales extremas como la suciedad, el calor y el frío.

Los access points (especificación reservada IP20) para montaje directo en rieles aéreos pueden ser utilizados para instalación en gabinetes de control. En este caso, las conexiones de antena son llevadas fuera del gabinete de control y las correspondientes antenas externas son usadas.
Gracias al calor y a la humedad se tienen los encapsulados resistentes a estos (IP65), estos dispositivos también pueden ser utilizados, por ejemplo, en entornos de frío intenso en cámaras de refrigeración. Y por supuesto, estos dispositivos se pueden situar en instalaciones externas, en condiciones extremas de frío, humedad o lluvia.

### 2.7.5 Seguridad en la WLAN

La seguridad en la red inalámbrica es tan importante como para las redes alámbricas. Particularmente el punto de transición desde una WLAN a LAN debe ser asegurado de modo que la WLAN no llegue a ser una puerta trasera para acceder a la red corporativa: esto es exactamente donde los datos corporativos sensibles que no deben caer en manos de personas no autorizadas.
Primero, es importante proteger la red de acceso entrante ilegal por personas o equipos externos.
Y segundo, medidas deben ser tomadas para prevenir la intercepción de datos.
Los últimos mecanismos de seguridad para redes WLAN basados en el estándar IEEE 802.11i con el algoritmo de seguridad mas potente WPA-2 dan protección contra los ataques al sistema empleando un proceso de autenticación mediante un servidor RADIUS (Remote Authentication Dial-In User Service) implementado en la red. Este servidor RADIUS es capaz de generar un par de llaves de encriptación para hacer imposible interceptar o escuchar datos en texto plano.
Además de estos mecanismos túneles VPN adicionales pueden hacer la comunicación más segura usando un gateway IPSec y los clientes correspondientes IPSec.

### 2.7.6 Entrada exitosa de la tecnología WLAN en aplicaciones industriales

Las ventajas que las WLAN ofrecen son obvias: gran flexibilidad, mejor movilidad y más conveniencia. La red inalámbrica es fácil de instalar y, comparada con las LAN cableadas, esta abre nuevas dimensiones – en aplicaciones industriales en particular. En fábricas y almacenes, por ejemplo, muchos escenarios de aplicación se pueden hacer posibles usando una WLAN. Y las conexiones inalámbricas siempre incrementan el trabajo seguro: un cliente wireless es definitivamente mas seguro y ciertamente mas conveniente que un cliente que deja un sendero de cable detrás de el.
En suma, las aplicaciones industriales cableadas usualmente requieren el uso de cables altamente flexibles y caros, y el cual tiene que ser reemplazado a intervalos regulares. Así que los puntos de la WLAN es aquí donde suben: la radiocomunicación no esta sujeta al diario “usa y rompe”.

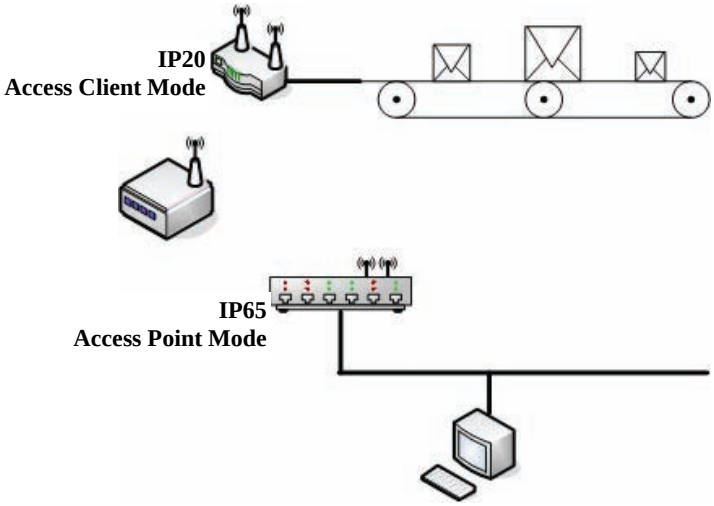



*Figura 2-40 Ejemplos de Aplicación en automatización industrial*

## 2.8 Comunicación segura en Ethernet

El propósito de los sistemas de seguridad es proteger la vida de humana y animal, maquinaria y el entorno. En automatización industrial los sistemas técnicos son requeridos lo cual permite salvaguardar estos sistemas de una forma automática. Tan pronto como un error es detectado en un sistema de seguridad, la falla del sistema de seguridad permanece en posición segura o cambia a una posición segura.

### 2.8.1 Estandarización – IEC 61508

Con el incremento de aplicaciones en sistemas de automatización también las demandas de seguridad relacionadas a las aplicaciones están creciendo. Cuando hablamos de seguridad tenemos que mirar el estándar IEC 61508. El estándar IEC 61508 describe la seguridad funcional de sistemas relacionados a la seguridad ya sean eléctricos / electrónicos / electrónicos programables. Este es un estándar genérico. Los estándares más específicos describen el uso de los sistemas relacionados a la seguridad. Actualmente están bajo desarrollo el estándar IEC 61511 relacionado a la industria del proceso y el estándar IEC 62061 relacionado a la automatización de la industria.
El estándar IEC 61508 se refiere al ciclo de vida entero de un sistema de seguridad. Así que la seguridad comienza con el diseño de un sistema y termina con el desmantelamiento y la eliminación.

Dentro de este estándar se describen los llamados “Safety Integrity Levels” (SIL). Estos niveles se encuentran desde el SIL 1 para el nivel mas bajo al SIL 4 para el nivel más alto y describen el grado de confianza en un sistema de automatización para cumplir su trabajo de una forma correcta basado en la tasa promedio de fallas continuas. Para las aplicaciones el SIL 3 es apropiado. Pero hay que tener cuidado, la clasificación SIL es solo un resultado de todos los componentes que se integran en un sistema. Si un “Programmable Electronic System” (PES; por ejemplo un PLC) es SIL 3 y el resto del bucle de control es SIL 2 entonces el bucle completo es solo SIL 2.

### 2.8.2 Reducción de riesgo

De acuerdo al estándar, seguridad significa que los riesgos tomados tienen que ser más bajos que el riesgo máximo tolerable. Esto significa que la idea básica del estándar es la reducción del riesgo.
El riesgo siempre significa una probabilidad de una situación riesgosa. El objetivo de un sistema de seguridad es reducir el riesgo, o en otras palabras reducir la probabilidad de una falla.

Esto se hace con funciones de diagnostico de alto nivel. La mayoría de las fallas son detectadas, pero en las menos hay probabilidad de que haya una falla oculta. Un ejemplo usual de dicho sistema en un sistema (valga la redundancia) donde dos procesadores en un PES calculan el mismo algoritmo de forma invertida y comparan los resultados. De ese modo, las fallas dentro de un procesador serán detectadas.

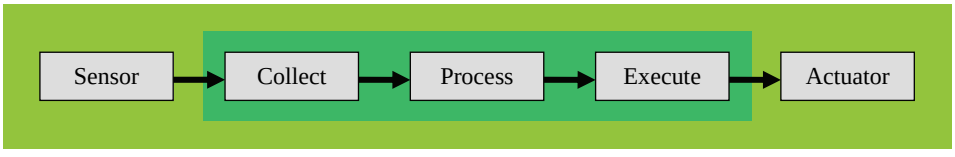



***Figura 2-41 Safety loop***

La probabilidad total de fallas en un sistema es la suma de todas las probabilidades de falla desde un sensor en un PES a un actuador. La parte oscura en la figura funciona en un PES (colecta, procesa, ejecuta). Este puede estar en una unidad. En una aplicación distribuida también puede pasar que la parte que colecta y/o la parte que ejecuta son procesadas en entradas/salidas remotas (RIO’s, Remote Input / Outputs).

En los sistemas modernos es también posible que la parte que procesa sea dividida en diferentes PES. Entonces la comunicación entre los dos PES también nos da una probabilidad de una alguna falla. El sistema completo consume 100% de la probabilidad de falla. Aquí se asume que el 15% de esta probabilidad es consumida por el PES completo. Dentro de ese PES la comunicación consume un 1% de la probabilidad de falla. Esto se muestra en la *Figura 55*.

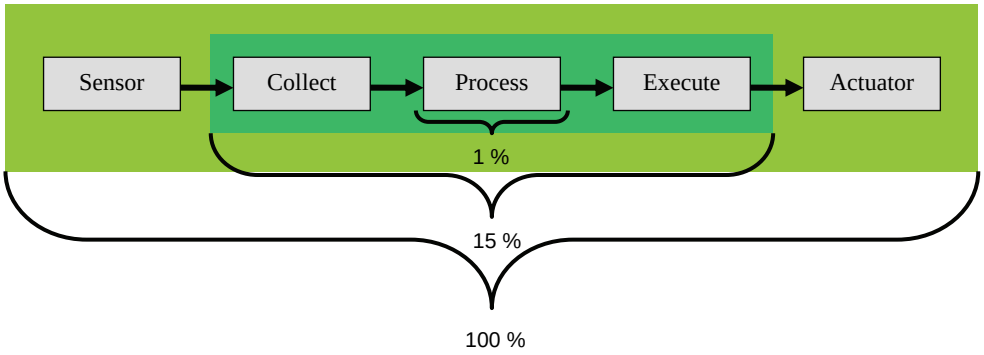



***Figura 2-42 Division de probabilidades***

Esto se tiene que distinguir entre el modo de baja demanda (probabilidad promedio de falla en demanda; PFD – Probability of Failure on Demand) y el modo de demanda continuo/alto (probabilidad de falla peligrosa por hora; PFH – Probability of Dangerous Failure per Hour).
La comunicación puede ser calculada en el modo de demanda continuo/alto. De acuerdo a la definición de SIL 3, el PFH tiene que estar entre $10^{-8}$ y $10^{-7}$. Esto significa que el PFH para la parte de la comunicación es solo una centésima parte de todo el PFH y, de este modo, entre $10^{-10}$ y $10^{-9}$.
Aun así Ethernet es muy robusto, esta tasa de falla tan baja no puede ser alcanzada por un Ethernet estándar.

### 2.8.3 Comunicación segura – *Canal Negro (Black Channel)*

Siempre es posible incluir cierto hardware en el cálculo de los valores del PFH. Pero por el otro lado, esto no tiene sentido para arreglar una comunicación a una plataforma de hardware.
Por ejemplo CAN es de uso probado. Es una muy buena y eficiente plataforma de hardware. Pero si la tasa de falla de CAN se incluye en el calculo PFH no es posible transferir datos seguros vía “Wireless CAN” sin recalcular los valores PFH de acuerdo a las diferentes tasas de error de bit.

Lo mismo es valido para la comunicación basada en Ethernet. Por lo tanto, tiene sentido poner un protocolo de alto nivel en la cima de la comunicación (Capa 7) y usar el resto de la comunicación (como pilas de software, hardware y transmisión) como un canal negro (black channel). En ese caso todos los componentes de infraestructura disponibles como cobre, fibra óptica, teléfono, satélite pueden ser usados.

En la siguiente figura se da la estructura de un PES*. El sistema de procesador redundante genera los datos relacionados a la seguridad. Estos datos son transferidos a otro compañero de comunicación segura vía una RAM de puerto dual, a un procesador de comunicación y a una infraestructura más o menos definida.

Los requerimientos para la infraestructura dependen de la aplicación. Si la infraestructura no es capaz de transmitir los datos en el tiempo especificado, el PES cambiara a la posición segura. En términos de seguridad, esto es un comportamiento correcto (pero no en términos de disponibilidad).
** Por razones de simplicidad el PES F30 de HIMA fue el ejemplo de esta estructura. El PES de otros vendedores se estructura y trabaja de manera similar.*

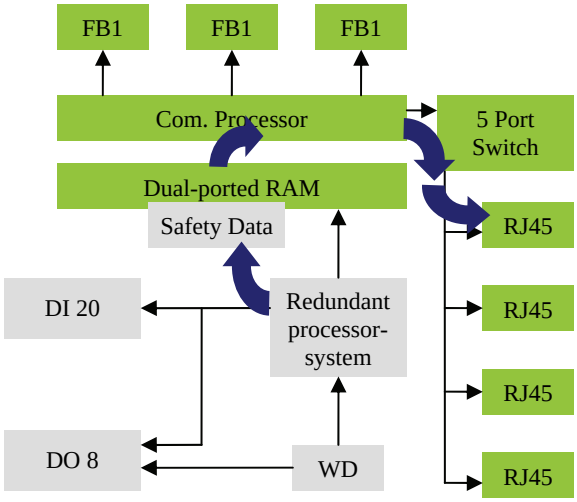



*Figura 2-43 Estructura Safe PES*

### 2.8.4 Generando un protocolo seguro

El protocolo Capa 7 tiene que eliminar todos los errores posibles. En la siguiente tabla se pueden ver diferentes métodos para evitar ciertos errores. Por ejemplo, un número secuencial ayuda a detectar iteración, pérdida, inserción y orden incorrecto de los datos. El requerimiento mínimo para un protocolo seguro es cubrir todos los errores mencionados.
Cada red tiene características especiales y modos de falla especiales (como el “hacer cola” o “queuing” en Ethernet). Así en adición a estos métodos se requiere un conocimiento profundo de la red utilizada.

### 2.8.5 Protocolo seguro basado en Ethernet

Aunque Ethernet es una excelente red este no sigue siendo capaz de dominar algunas reglas de aplicaciones de seguridad. Las aplicaciones de seguridad necesitan un manejo seguro de los datos. Esto quiere decir que el ajuste de los parámetros de comunicación tiene que ser hecho de una manera segura. No es posible usar DHCP (o protocolos similares) para ajustar las direcciones IP. DHCP no es un protocolo seguro y también el servidor que maneja el DHCP no tiene una certificación SIL. Las ventajas de TCP son inútiles. El mecanismo de control de la conexión no puede utilizarse relacionado a la seguridad. Esto tiene que hacerse en el nivel de comunicación más alto (Capa 7).

En una segunda mirada veremos que esto no es una limitante para Ethernet. Es práctico que estos tópicos se analicen en relación con Ethernet y aquellos servicios que están disponibles para dispositivos no seguros. Del otro lado, si se tiene un servidor de direcciones SIL adaptado y una comunicación SIL adaptada se pueden asignar direcciones IP, distribuir programas, etc.
Si toda esta comunicación es compatible con los estándares Ethernet entonces la red Ethernet es una plataforma poderosa para aplicaciones relacionadas a la seguridad.

Las siguientes son solo algunas ventajas de Ethernet que serán enfatizadas de tal forma que se ayude a que el sistema sea seguro de forma especial.

| | Métodos | | | | | |
|---|---|---|---|---|---|---|
| Error | Numero Secuencial | Estampa de tiempo | Noticia de recepción | Identific. de emisor y receptor | Copia de seguridad de datos | Redundancia con comparación cruzada |
| Iteración | X | X | | | | X |
| Pérdida | X | | X | | | X |
| Inserción | X | | X | X | | X |
| Orden incorrecto | X | X | | | | X |
| Mensaje corrupto | | | X | | X | |
| Retardo | | X | | | | |
| Conexión Segura y No-Segura | | | X | X | | |

***Tabla 2-8 Posibles errores y métodos para evitarlos***

### 2.8.6 Robustez

La práctica indica que Ethernet es capaz de conseguir resultados importantes en el entorno industrial. Por ejemplo, la calidad de una comunicación Ethernet ha sido probada en una fábrica de autos alemana. Al tener los peores casos de condiciones electromagnéticas en un cable Ethernet de 100 metros que ha sido colocado en un área de soldadura con bucles arriba de los transformadores (en vez de una instalación fija). Dentro de 16 días de pruebas se transfirieron 538, 562,446 mensajes (como medio billón de mensajes). De estos se transfirieron 389.5 por segundo. Del total de mensajes solo 15 fueron afectados en la red. Estos errores se detectaron con el PES. Esto muestra que aun el Ethernet estándar se adecua a los requerimientos de la automatización industrial.

#### 2.8.6.1 *Una instalación*

Incluir un sistema de seguridad resulta en altos costos de instalación. Adicionalmente, en las instalaciones actuales con frecuencia dos o más sistemas fieldbus son utilizados. Uno (o mas) para comunicación estándar y uno para comunicación de seguridad. Ethernet ofrece un gran ancho de banda. Este gran ancho de banda debería también ser usado para la comunicación de seguridad.
Los requerimientos con respecto al retraso o delay (tiempo real) y a la fluctuación o jitter (determinismo) de los mensajes son casi siempre llenados por con un Ethernet estándar (o aun llenados por protocolos Ethernet de tiempo real como se describió en los subcapítulos anteriores).
Una premisa para usar una red para diferentes comunicaciones es la coexistencia de diferentes protocolos en una red. Por lo tanto, safeethernet (un protocolo seguro sobre Ethernet) usa tramas UDP estándar con datos seguros incluidos en la Capa 7.

El propósito de una maquinaria o planta producir un gran numero de productos de una calidad deseada. Por lo tanto, el usuario siempre trata de aumentar la disponibilidad. El mal funcionamiento es una de las razones para los tiempos de producción muertos. Otra razón es que ningún tipo de seguridad descansa. Lo mas complejo de la maquinaria es detallar la información de diagnostico que tiene que estar cuando se tenga que reiniciar. Ethernet es capaz de ofrecer acceso total a todos los dispositivos en la red desde cada puerto en la misma. Así la información proporcionada al sistema de seguridad esta disponible donde se quiera que este disponible. Y una vez mas, Ethernet switcheado ofrece ancho de banda de reserva para transmitir estos datos seguros.

#### 2.8.6.2 *Velocidad en sistemas descentralizados*

Cuando se piensa en la velocidad de la comunicación, Ethernet ofrece algunas ventajas. Una ventaja poco mencionada es que el ancho de banda completo siempre esta disponible. Si un dispositivo solo ofrece 10 MBits entonces el resto de la red puede seguir comunicándose a 100 MBits o 1 Gbit.
Si dispositivos descentralizados se utilizan para colectar datos y leen las señales de salida dos veces el tiempo de comunicación tiene que ser sumado.

El margen de seguridad de un proceso peligroso depende directamente del tiempo de reacción del sistema de seguridad (la suma del tiempo del sensor, colección, proceso, ejecución y actuador). Así el tiempo de reacción mas rápido es, el menor espacio que es necesario en la planta.
La velocidad es un método para asegurar dinero. El tiempo de comunicación se transforma en el elemento mayor de todo el concepto de seguridad.

### 2.8.7 El futuro de la seguridad relacionada a la comunicación

En el futuro conceptos modulares como la “swap” de los dispositivos mecatronicos durante la operación de la maquina serán creados. Es posible llevar la PES directamente a elementos rotativos y conectarlos vía Wireless LAN. Debido a la profunda información de diagnostico es posible localizar el error desde cualquier parte de la red.

Esto también posibilita mejores diagnósticos remotos. Esto debería tenerse en mente ya que la seguridad juega un papel muy importante en el acceso remoto. Esto también influencía a las aplicaciones de seguridad. Al momento el estándar IEC 61508 no cubre este tema, pero un grupo de trabajo ya comenzó a encontrar comparaciones de seguridad y niveles de la misma.

Como estos conceptos están creciendo es necesario apoyar estas tecnologías de una manera segura y no segura. Ethernet es la plataforma de comunicación disponible que soporta los requerimientos de las características futuras.

# CAPITULO 3

## Protocolos industriales Ethernet selectos y aplicaciones

## 3.1 Visión general de algunos protocolos industriales Ethernet

Causada por una promoción muy fuerte de varias compañías y organizaciones, una variedad de protocolos industriales basados en Ethernet han sido desarrollados en los últimos años.
La Comisión Internacional Electrotécnica (IEC, International Electrotechnical Comission) ha aceptado recientemente 10 propuestas de protocolos basados en Ethernet como IEC/PASs (Publicity Available Standards) mostrados en la *Tabla 3-1*, la cual pone estas especificaciones en pista de aprobación como estándares IEC internacionales los cuales están planeados para arrancar en 2007 (en el contenido de IEC 61158 e IEC 61784). Además de las especificaciones conocidas ya listas, un par de nuevos protocolos aparecen los cuales principalmente vienen de compañías asiáticas (EPA, TCnet, Vnet/IP) las cuales están basadas en la tecnología fieldbus existente (P-NET), o las cual contienen algunas extensiones (Modbus-RTPS). Los 10 protocolos y otros considerando sus similitudes y diferencias serán presentados en este capitulo en breve.

| Nombre de la Especificación | Standard IEC |
|---|---|
| EPA | IEC/PAS 62409 |
| EtherCAT | IEC/PAS 62407 |
| EtherNet/IP | IEC/PAS 62413 |
| ETHERNET Powerlink | IEC/PAS 62408 |
| Modbus-RTPS | IEC/PAS 62030 |
| P-NET on IP | IEC/PAS 62412 |
| PROFINET IO | IEC/PAS 62411 |
| SERCOS III | IEC/PAS 62410 |
| TCnet | IEC/PAS 62406 |
| Vnet/IP | IEC/PAS 62405 |

***Tabla 3-1 (Pre-) Standards Protocolos Industriales basados en Ethernet***

### 3.1.1 EPA

EPA (Ethernet for Plant Automation) fue desarrollado por la compañía china **Supcon** y es un nuevo enfoque para soportar comunicaciones deterministicas para aplicaciones distribuidas basadas en TCP/IP o UDP/IP y un mecanismo de time slot. El mecanismo es realizado con el ECSME (EPA Communication Scheduling Management Entity) la cual es una extensión de la capa de link de datos (Capa 2) la cual se representa en la *Figura 3-1*.

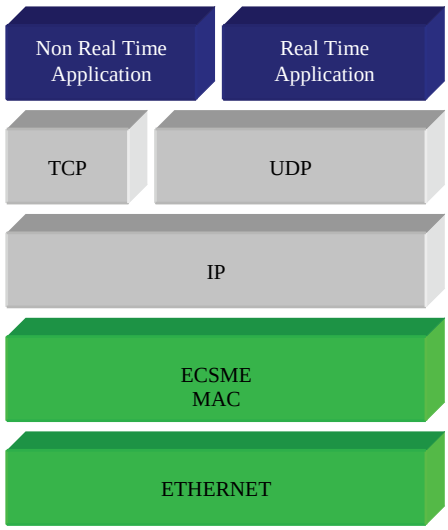



***Figura 3-1 Pila EPA***

Un macro-ciclo de comunicación es dividido en dos fases: una fase de de transferencia de mensaje periódico y una fase de transferencia de mensaje no-periódico.

El proceso de aplicación puede ser explorado a este modelo de comunicación con el “EPA Function Block Application Process (una aplicación de control en tiempo real) y un proceso de aplicación que no corre en tiempo real el cual corre en estándares de Ethernet y TCP/IP o UDP/IP.
Se espera que un macro-ciclo en un múltiplo de milisegundos pueda ser conseguido para la sincronización de mecanismos de relojes distribuidos basados en el estándar IEEE 1588.

### 3.1.2 EtherCAT

EtherCAT (Ethernet for Control Automation Technology) es el concepto de automatización en tiempo real basado en Ethernet desarrollado por la compañía alemana **Beckhoff**. Fundado a finales del 2003 en el ETG (EtherCAT Technology Group) tiene más de 180 miembros.
En contraste a las otras soluciones basadas en Ethernet, el paquete Ethernet tan pronto es recibido, es entonces interpretado y copiado como proceso de datos a cada dispositivo dentro de la red.
En vez de eso, la trama Ethernet es procesada al vuelo: para cada modulo dentro de la red, la dirección de datos de ese dispositivo es leída, mientras el telegrama es re-enviado al siguiente aparato. Similarmente, datos de entrada son insertados mientras el telegrama pasa a través del dispositivo. Los telegramas son retrasados por un aparato por unos cuantos nanosegundos los cuales deberían dar un incremento del rendimiento del sistema comparado con las otras soluciones basadas en Ethernet.
El último dispositivo del segmento de red envía la trama de regreso para crear una estructura lógica y física en anillo. Los datos transferidos comprenden tramas Ethernet compatibles, dentro del segmento de la red estas tramas son convertidas a un bus interno (E-Bus) el cual será procesado por cada esclavo.

Las tramas Ethernet de tiempo real tienen prioridad sobre otros datos (como aquellos que se requieren para configuración o diagnostico, etc.) vía un sistema interno de priorización. Los datos de configuración son transmitidos en el tiempo entre tramas si el tiempo suficiente esta disponible o usando un canal específico de servicio. La totalmente mantenida funcionalidad Ethernet del sistema operativo logra compatibilidad con los protocolos IP convencionales.

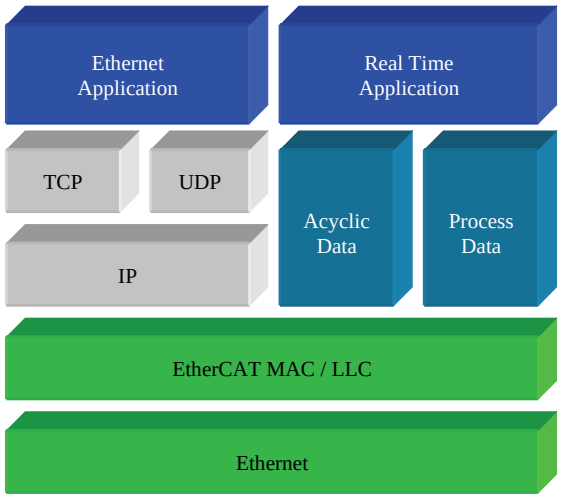



***Figura 3-2 Pila EtherCAT***

Los mecanismos de sincronización basados en el estándar IEEE 1588 logran un rendimiento capaz de soportar aplicaciones de control de movimiento y seguridades relacionadas a aplicaciones arriba del SIL 4 pueden ser logradas con EtherCAT. Controladores esclavos y ASICs están disponibles a partir de la segunda mitad del 2005.

### 3.1.3 EtherNet/IP

EtherNet/IP, basado en Ethernet TCP o UDP IP, es una extensión de pila para la comunicación en la industria de la automatización. La IP en EtherNet/IP quiere decir Protocolo Industrial (IP, Industrial Protocol). EtherNet/IP fue introducido por la ODVA (Open DeviceNet Vendor Association) hacia finales del año 2000, desarrollando y especificando el trabajo que es logrado por los SIGs (Special Interest Groups). ODVA tiene más de 300 miembros alrededor del mundo, un laboratorio de conformidad y pruebas es manejado por la Universidad de Magdeburgo en Alemania.

Básicamente en EtherNet/IP el Protocolo superior de Control e Información (CIP, Control and Information Protocol) el cual es ya usado en ControlNet y DeviceNet es adaptado al Ethernet TCP/IP y UDP/IP respectivamente. La especificación de EtherNet/IP es publica y libre de cargo en el sitio Web de ODVA. En suma a las aplicaciones típicas de oficina como HTTP, FTP, SMTP y SNMP, EtherNet/IP provee un servicio Productor/Consumidor permitiendo la transmisión de mensajes de tiempo-critico entre el controlador y los módulos de E/S.

La transmisión de datos seguros de mensajes no-cíclicos (inicio de programa/descarga, configuración) serán realizados usando TCP y la transmisión de tiempo-critico de los datos de control cíclico serán manejadas por la pila UDP. Perfiles de dispositivos estándar como válvulas neumáticas o controles de movimiento están disponibles también.

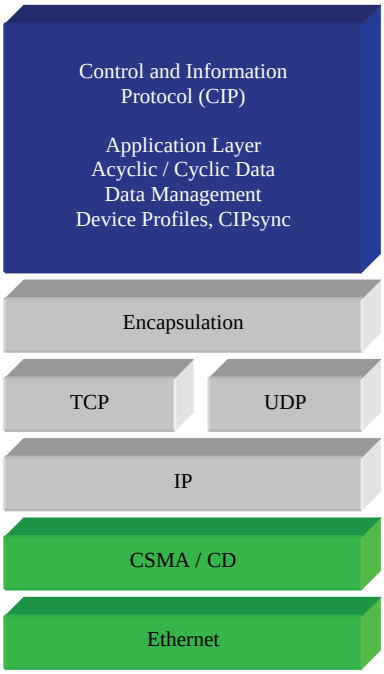



***Figura 3-3 Pila EtherNet/IP***

El protocolo CIP actualmente esta siendo extendido para los requerimientos de seguimiento en tiempo real y seguridad. CIPsync es una extensión que realiza mecanismos de sincronización de tiempo en sistemas distribuidos usando un método basado en el estándar IEEE 1588 mientras que CIPsafety es una extensión que integra mecanismos de seguridad y habilita sistemas de control de seguridad basados en Ethernet/IP hasta SIL 3. Ambas extensiones están actualmente bajo desarrollo. Los primeros productos para CIPsafety fueron anunciados en el 2005 y para CIPsync en el 2006.

### 3.1.4 ETHERNET Powerlink

Originalmente ETHERNET Powerlink (EPL) había sido desarrollado por la compañía austriaca Bernecker + Rainer (B&R). Después de la publicación del estándar ETHERNET Powerlink en abril del año 2002, ahora B&R esta trabajando junto a compañías y organizaciones como Hirschmann, Lenza, Kuka y la Universidad de Zurich de Ciencia Aplicadas Winterthur como coordinador del Grupo de Estandarización ETHERNET Powerlink (EPSG, ETHERNET Powerlink Standardization Group).
Este consorcio mejorara el estándar ETHERNET Powerlink para cumplir los requerimientos de drives síncronos (control de movimiento) y otros dispositivos específicos. Por ejemplo, los mecanismos de sincronización basados en el estándar IEEE 1588 serán implementados.

En ETHERNET Powerlink las pilas estándar TCP y UDP/IP en la capa 3 y 4 son extendidas como sigue:

Un agregado entre las capas 2 y 3 para la transferencia de datos asíncrona y entre las capas 2 y 7 es implementado otro para la transferencia de datos rápida, cíclica e isócrona, de este modo da canales de comunicación diferentes para diferentes datos de comunicación (en tiempo-real y no-real).

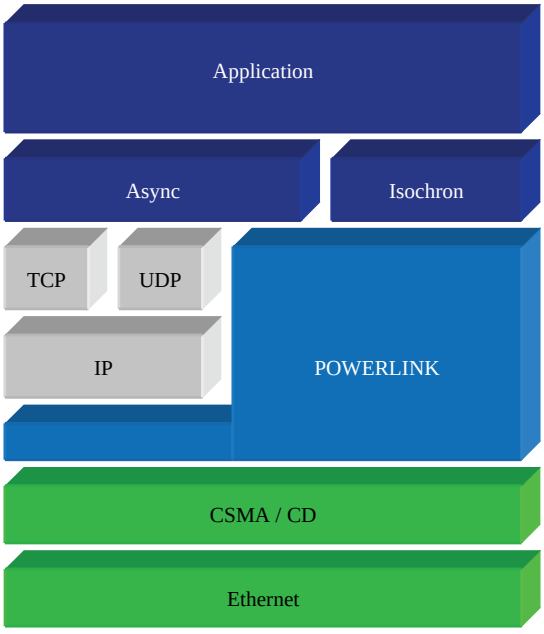



***Figura 3-4 Pila Powerlink***

La pila ETHERNET Powerlink controla completamente el tráfico de datos en la red. El método es llamado Manejo de Red por Slot de Comunicación (SCNM, Slot Communication Network Management) y dará capacidad de tiempo-real sobre Ethernet. Cada estación tiene muy limitado el tiempo y los derechos de comunicación y puede enviar datos a cada estación dentro de la red.
En un tiempo muy particular solo una estación puede acceder al bus y así las colisiones son imposibles y de esta manera se mejora el rendimiento deterministico.
Sumados a este slot de tiempo para la transferencia de datos isócrona, el SCNM provee slots de tiempo comunes para transferencia de datos asíncrona.

Además las extensiones contendrán mecanismos de sincronización de tiempo basados en el estándar IEEE 1588 y aplicaciones relacionadas de seguridad que serán cubiertas por la especificación EPLsafety la cual debería de llenar los requerimientos del SIL 3 (dentro de una arquitectura específica también el SIL 4). Además, EPL versión 2 contiene comunicación basada en CANopen y perfiles de dispositivos.

### 3.1.5 JetSync

La compañía alemana Jetter ofrece un método de sincronización vía Ethernet TCP/IP el cual se llama JetSync. Este usa una tecnología similar a IEEE 1588 pero también soporta comunicación asíncrona. La compañía afirma que su sistema encabeza a una estructura mas abierta y flexible que se consigue usando estrictos métodos de sincronización de time-slot.

JetSync soporta aplicaciones de control de movimiento así como transmisión de datos ordinarios asíncronos a través de TCP/IP. Esto, dice la compañía, consigue compatibilidad usando componentes estándar para comunicación entre PLC's, drives, módulos de E/S y componentes SCADA. Jetter afirma que la sincronización de ejes de movimiento se puede mejorar a más de 10μs de fluctuación solo usando TCP/IP corriendo solo en una infraestructura Ethernet estándar.

### 3.1.6 Modbus-RTPS

El grupo Modbus-IDA (con base en E.U.) esta trabajando hacia un desarrollo mayor de la arquitectura IDA para sistemas de control distribuido usando Modbus/TCP y RTPS para propósitos de comunicación. Modbus/TCP es un derivado del protocolo Modbus y fue desarrollado por Modicon (Schneider Electric), la especificación fue publicada en 1999 y esta disponible en Internet libre de cargos. Al lado de las actividades de la IEC la especificación ha sido presentada a la IETF (Internet Engineering Task Force) para introducir este al estándar Internet. Esto quiere decir que por ejemplo Modbus/TCP como FTP podría ser implementado en todos los sistemas operativos comunes.

Modbus/TCP esta basado en Ethernet y en el estándar TCP/IP y esta montado directamente en la capa 4 (TCP/UDP) usando el puerto 502. Este define una estructura simple y protocolo abierto y ampliamente utilizado para una comunicación maestro-esclavo. Un concepto extenso de la arquitectura no existe, básicamente un telegrama Modbus esta incrustado en las tramas de la capa inferior (TCP, IP, etc.) y transferido vía el medio físico.

El telegrama Modbus contiene la dirección del esclavo, el código de función Modbus, los datos a ser transferidos un checksum el cual no será usado aquí debido a los mecanismos de detección de errores de las capas inferiores (Capas 1-4). El código de función representa la acción que el esclavo tiene que efectuar. De una manera simple un esclavo compatible con Modbus/TCP (por ejemplo un modulo de E/S) puede ser controlado con un pequeño numero de funciones Modbus. Debido a que el Modbus/TCP es el mas viejo de los protocolos industriales basados en Ethernet el numero de los dispositivos disponibles usando este protocolo es muy alto.

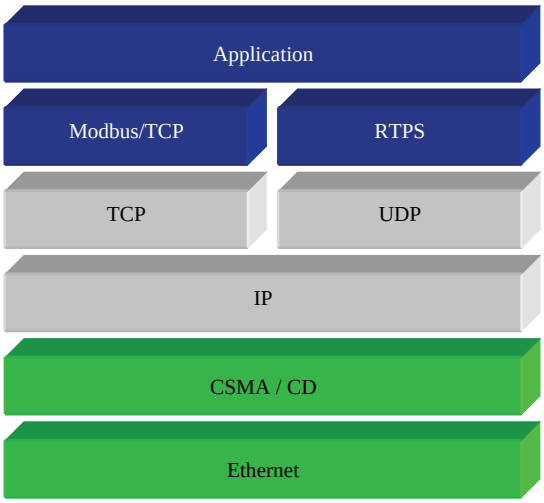



*Figura 3-5 Pila Modbus-RTPS*

Al lado de la especificación del protocolo para una comunicación maestro-esclavo, la IEC/PAS proporciona el protocolo RTPS (Real-Time Publish Suscribe) el cual permite comunicación multicast (multidifusión) usando el estándar UDP/IP, por ejemplo para la sincronización de aplicaciones distribuidas. Características requeridas del protocolo como son el determinismo y la confiabilidad serán la responsabilidad en el mediano plazo para implementar este protocolo.

### 3.1.7 P-NET on IP

P-NET on IP esta basado en el fieldbus danés P-NET existente (estándar europeo EN desde 1996) el cual es promovido y mantenido por la IPUO (International P-NET User Organisation).

La especificación P-NET on IP esta diseñada para usarse en un entorno IP. P-NET on IP permite el uso de la comunicación P-NET de tiempo-real envuelto en paquetes de comunicación UDP/IP.
Para la especificación del telegrama usado, los puerto UDP 34378 para comunicación P-NET normal y el puerto 34379 para comunicación segura P-NET serán utilizados por este protocolo, donde un mensaje usando el último puerto requerirá la introducción de un password.

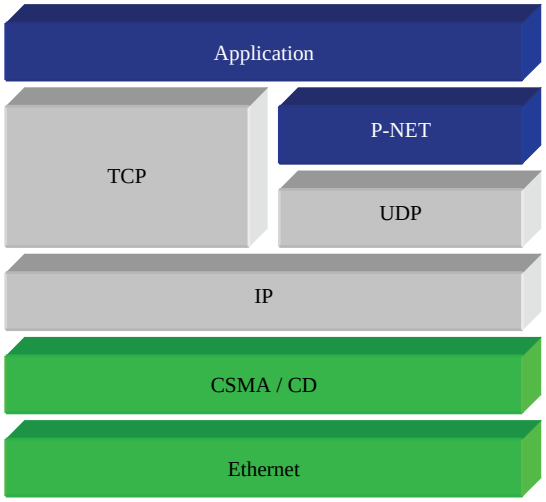



***Figura 3-6 Pila P-NET***

Las extensiones P-NET on IP al actual estándar P-NET incluye una descripción de la estructura de los paquetes UDP/IP para los mensajes P-NET. Esto mejora las actuales definiciones de los modos de direccionamiento de mensajes P-NET (por ejemplo sencillo, extendido, complejo) con IP, incluyendo definiciones de ruteo. Implementación de P-NET on IP para Ethernet de Tiempo-Real, significa que los paquetes P-NET pueden ser ruteados a través de redes IP, en exactamente la misma vía que si estos fueran ruteados a través de redes no-IP.
El ruteo puede ser a través de cualquier red del tipo P-NET y en cualquier orden. Los nodos en una red IP son direccionados con dos elementos de ruteo P-NET, pero esto es enteramente manejado por los nodos IP. Esto quiere decir que cualquier cliente P-NET (master) puede acceder a servidores en una red IP, sin conocer nada acerca de las direcciones IP.

### 3.1.8 PROFINET

PROFINET fue desarrollado por la PNO (Profibus Nutzer/User Organisation) con soporte muy fuerte de Siemens y esta disponible desde 2002. La primera versión de PROFINET uso Ethernet para comunicación de tiempo No-critica de dispositivos de alto nivel y tecnología de fieldbus Profibus-DP para dominios de tiempo-real integrados a un alto nivel por proxys.

En su segunda versión PROFINET proporciono dos mecanismos de comunicación sobre Ethernet:

El canal de comunicación estándar de tiempo-no-real usa TCP/IP mientras un segundo canal deriva la Capa 3 y 4 del modelo de referencia OSI brinda comunicación más deterministica. El protocolo reduce el largo de los datos para minimizar el tiempo de throughput en la pila de comunicación. Para un optimo rendimiento de comunicación PROFINET prioriza el paquete como es especificado en el estándar IEEE 802.1. Para comunicación de tiempo-real (RT, Real-Time) la prioridad más alta (prioridad 7) será utilizada.

PROFINET Versión 3 usa una solución de hardware para derivar el canal rápido basado en software reduciendo el throughput time en la pila de comunicación todavía adicional.
En conexión con switcheo Ethernet PROFINET V3 da una solución muy rápida basada en Tiempo-Real Isócrono (IRT, Isochronous Real Time) el cual satisface los requerimientos de las aplicaciones de control de movimiento.

Todos los mecanismos de comunicación provistos por PROFINET pueden ser usados en los siguientes modos:

1. PROFINET IO para la integración de E/S distribuidas (comunicación RT e IRT).
2. PROFINET CBA o Automatización Basada en Componente (Component Based Automation) que usa comunicación vía TCP/IP y RT; para la creación de plantas modulares.

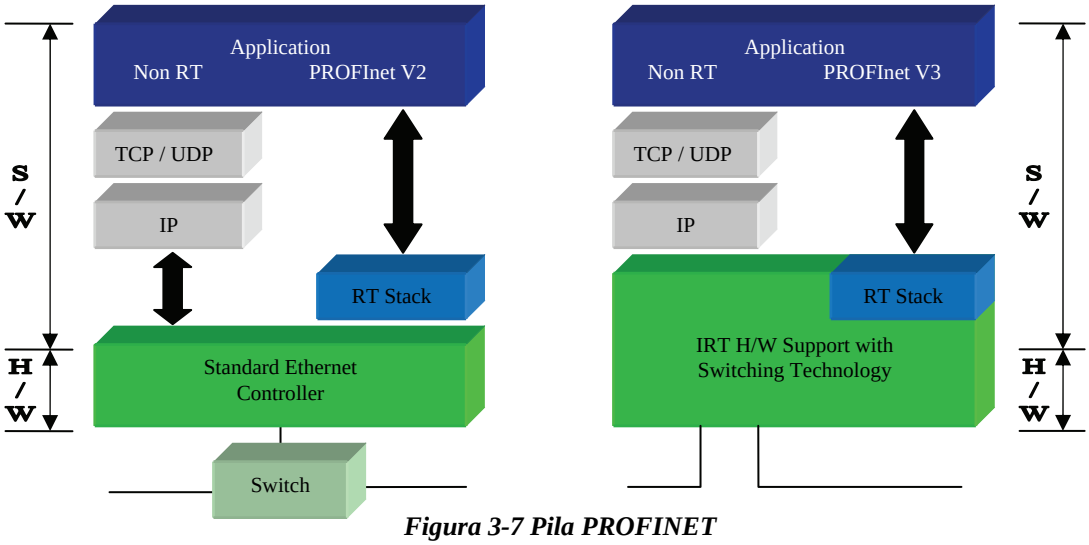



***Figura 3-7 Pila PROFINET***

PROFINET y también extensiones relacionadas a aplicaciones de seguridad (safety applications) llamado PROFIsafe están actualmente bajo desarrollo, las primeras aplicaciones están listas y disponibles desde finales del 2005.

### 3.1.9 SERCOS III

SERCOS (SErial Real-Time COmmunication System) ha sido desarrollado por un consorcio industrial en cooperación con ZVEI y VDM en los ‘80s. Marketing, además de trabajo de desarrollo y actividades de estandarización están bajo responsabilidad del IGS (Interest Group SERCOS interface) el cual fue fundado en 1990.

Después la interfaz SERCOS ha sido aprobada como un estándar internacional en 1995 (IEC 61491), además los pasos de desarrollo toman lugar dentro de la segunda generación de SERCOS, por ejemplo incrementando la tasa de transferencia.

Comportamiento de Tiempo-Real y determinismo serán logrados usando mecanismos de time-slot (Time Division Multiplex Access o TDMA) y sincronización de hardware. Los time-slots permiten transmisión transmisiones de datos de tiempo-critico y no-critico en alternancia. SERCOS fue originalmente desarrollado como interfaz de manejo pero incluye módulos convencionales de E/S a los dispositivos soportados.
La tercera versión, SERCOS III ha sido diseñada para Ethernet industrial. Además las extensiones incluyen reemplazo del hardware basándose en interfaces de comunicación con soluciones más flexibles, por ejemplo en el soporte de diversos protocolos de automatización basados en software y el uso de componentes de hardware estándar (links Ethernet en vez de links de fibra óptica).

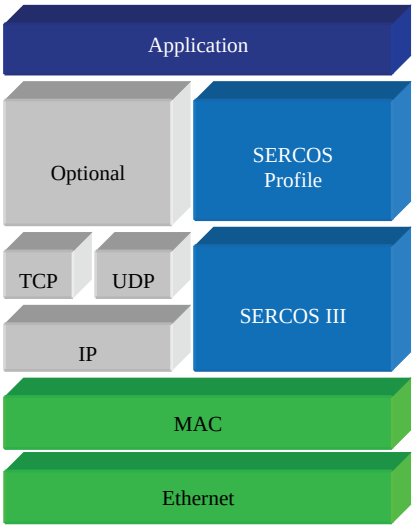



***Figura 3-8 Pila SERCOS***

### 3.1.10 TCnet

La red de Control de Tiempo-critico basada en Ethernet (TCnet, Time-critical Control Network) es la propuesta que la compañía japonesa Toshiba da para la transmisión de datos en tiempo real (cíclica) y un servicio de mensaje de datos asíncrono. La extensión de tiempo real esta localizada en la Capa MAC y es llamada DOMA (Deterministic Ordered Multiple Access) proveyendo funcionalidades para evitar colisiones en el medio con una respuesta de tiempo definida.
La transmisión de datos cíclica involucra tres modos de velocidad: alta, media y baja velocidad las cuales pueden ser asignadas de acuerdo a la actualización del ciclo de datos. La transmisión normal de mensajes soporta el canal estándar TCP/IP y UDP/IP. La capa de servicio de aplicación TCnet define un sistema de memoria común el cual se comparte sobre la red TCnet por la aplicación participante en cada dispositivo.

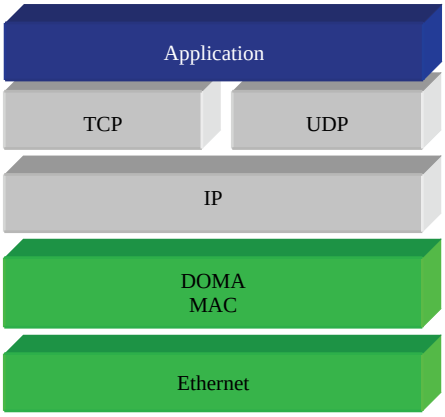



***Figura 3-9 Pila TCnet***

### 3.1.11 Vnet / IP

Vnet / IP es un sistema de red de planta en tiempo real para automatización de procesos continuos y en grupo y fue desarrollado por la compañía japonesa Yokogawa. Datos de tiempo-no-critico (datos de ingeniería y mantenimiento) para comunicación con PC's, subsistemas y HMI (Human Machine Interface) son enviados vía TCP/IP, datos de control de tiempo-critico son enviados vía UDP/IP.
El concepto proporciona interfaces para fieldbuses subyacentes como son Modbus/TCP o DeviceNet. En el perfil de la pila Vnet /IP una capa de transporte especifica de tiempo-real para aplicaciones de control llamada RTP (Real-time & Reliable Datagram Protocol) es implementada usando el canal UDP/IP.

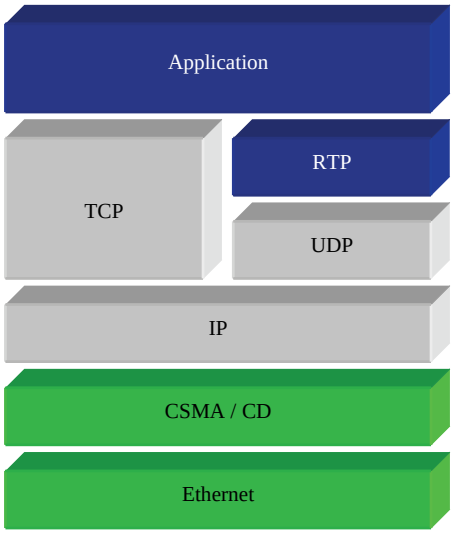



***Figura 3-10 Pila Vnet/IP***

Tecnologías como esquemas de priorización, rendimiento en tiempo-real en el rango de milisegundos pueden ser conseguidas con Vnet / IP. Para aplicaciones estándar de IT como son FTP y HTTP, el canal de comunicación TCP/IP es utilizado. Además, la red puede ser hecha con doble redundancia para instantáneamente cambiar a otra trayectoria de red si una trayectoria de red falla, mejorando la fiabilidad del sistema de control.
Vnet / IP esta implementado dentro de las series CENTUM de Yokogawa la cual cubre el mercado de sistemas de control distribuido.

### 3.1.12 Protocolos adicionales

En suma a los protocolos descritos anteriormente, más aplicaciones Ethernet como son FTE, HSE, RTnet, safeethernet, SynqNet, SynUTC están disponibles.

- El *FTE* (Fault Tolerant Ethernet) de Honeywell es un protocolo industrial basado en Ethernet para control de procesos basados en IP actuando para la detección de fallas y recuperación para manejo de puntos múltiples de fallas de red y soporta comunicaciones con dispositivos nativos no-FTE.
- *HSE* (High Speed Ethernet) esta soportado por la Fieldbus Foundation. Desde un punto de vista técnico HSE opera como un backbone y esta interconectado con el sistema de fieldbus subyacente (bus H1) vía gateways.
- *RTnet* es una pila de protocolo de red en tiempo real de código abierto para RTAI (Real-Time Linux Extension), fue desarrollado por la Universidad de Hanover, y esta basado en hardware Ethernet estándar y una Capa MAC modificada.
- Como un producto de la compañía alemana HIMA, el protocolo *safeethernet* usa una red basada en Ethernet estándar y por lo tanto permite la aplicación la aplicación de protocolos estándar de IT's.

Recientemente HIMA ha presentado un convertidor Ethernet-Ex permitiendo la aplicación de componentes Ethernet en Ex Zone1.
- El *SynqNet* abordado, promovido y mantenido por Danaher y el SynqNet User Group, es un protocolo basado en Ethernet para aplicaciones de control de movimiento basado en una modificada Capa de Link de Datos y una implementación dedicada de la Capa 3 a la 7. Aquí no hay compatibilidades con protocolos estándar de IT's.
- La tecnología *SynUTC* (Synchronised Universal Time Coordinated) basada en Ethernet fue desarrollada por Oregano Systems y ofrece tolerancia a las fallas y alta exactitud en la sincronización de tiempo basado en el estándar IEEE 1588 usando protocolos de red estándar.

En la siguiente tabla se muestran algunas de las características de los protocolos considerados anteriormente.

| | Arquitectura | Requerimientos de Hardware | Comportamiento de Tiempo *) | Mas Información en |
|---|---|---|---|---|
| EPA | Abierta | Capa MAC Modificada | Multiple de milisegundos | www.epa.org.cn (solo en Chino) |
| EtherCAT | Subset de Tiempo real | Hardware especifico (ASICs) | Ciclo: 100 μs para 100 drives sincronizados | www.ethercat.org |
| EtherNet/IP y CIPsync | Abierta | Standard, CIPsync: Hardware IEEE 1588 | Ciclo: 300/330 μs @ 30 drives sincronizados, Disparo: 100 ns (con CIPsync) | www.odva.org www.ethernetip.de |
| ETHERNET Powerlink | Subset de Tiempo real | Standard | Ciclo: <100 μs, Disparo: <1 μs | www.ethernet-powerlink.com |
| JetSync | Abierta | Standard | Ciclo: <5 ms, Disparo: <10 μs | www.jetter.de |
| Modbus-RTPS | Abierta | Standard | Ciclo: approx. 5-10 ms | www.modbus-ida.org |
| P-NET on IP | Abierta | Standard | No disponible | www.p-net.org |
| PROFInet | Subset de Tiempo real | Standard / ASICs (con Switch) | Ciclo: 5-20 ms (V2), 1 ms (V3), Disparo: 1 μs @ 100 drives sincronizados | www.profibus.com |
| SERCOS III | Subset de Tiempo real | Dedicado (FPGA) | Ciclo: 31.25 μs @ 10 drives sincronizados, 250 μs @ 100 drives, Disparo: <1 μs | www.sercos.de |
| TCnet | Abierta | Capa MAC modificada | Ciclo: 1 ms | www.toshiba.com |
| Vnet/IP | Abierta | Standard | Ciclo: 10 ms | www.yokogawa.com |
| *) Valores dados por los fabricantes | | | | |

***Tabla 3-2 Características de algunos Protocolos Industriales basados en Ethernet***

## 3.2 EtherCAT

### 3.2.1 Introducción: Ethernet y la capacidad de tiempo-real

Hay muchas propuestas que intentan dar una capacidad de tiempo real para Ethernet: por ejemplo, el procedimiento de acceso a la media CSMA/CD esta deshabilitado vía las capas mas altas del protocolo y reemplazado por el procedimiento de trozo de tiempo o poleo, otras propuestas usan switches que distribuyen los paquetes Ethernet en una manera precisa de control del tiempo.
Mientras estas soluciones pueden ser capaces de transportar paquetes de datos de forma más o menos rápida y exacta a los nodos Ethernet conectados, los tiempos requeridos para la redirección a las salidas o controladores y para la lectura de los datos de entrada dependen de la implementación.

Si tramas individuales Ethernet son usadas por cada dispositivo, la tasa de datos utilizable es más baja en principio: La trama Ethernet mas pequeña tiene 84 bytes de longitud (incluyendo el paquete inter-tramas IPG). Si por ejemplo un drive manda cíclicamente 4 bytes de valor actual e información de estado y en consecuencia recibe 4 bytes de valor de comando y palabra de control de información, un 100% de la carga del bus (por ejemplo con tiempo de respuesta infinitamente pequeño del drive) una tasa utilizable de solo 4/84 = 4.7% es alcanzada. En un tiempo de respuesta promedio de 10 μs, la tasa disminuye a 1.9%. Estas limitaciones aplican a todas las aproximaciones Ethernet que envían una trama Ethernet a cada dispositivo (o esperan una trama de cada dispositivo), sin distinción de los protocolos usados dentro de la trama Ethernet.

### 3.2.2 Principio de operación EtherCAT

La tecnología EtherCAT supera las limitaciones inherentes de otras soluciones Ethernet: el paquete Ethernet ya no es recibido, entonces interpretado y los datos del proceso después copiados a cada dispositivo. Los dispositivos esclavos EtherCAT leen los datos direccionados a ellos mientras la trama pasa a través del nodo. Similarmente, el dato de entrada es insertado mientras el telegrama pasa. Las tramas solo se retrasan unos pocos nanosegundos. Ya que la trama de datos consta de muchos dispositivos en las direcciones de envió y recepción, la tasa de datos utilizable se incrementó hasta el 90%. Las características full-duplex de 100Base-TX son completamente utilizadas, así que la tasa efectiva de datos que se puede lograr es mayor a 100 Mbps (>90% de 2X100 Mbps).
El protocolo Ethernet de acuerdo al estándar IEEE 802.3 continua intacto en las terminales individuales, ningún sub-bus es requerido.

### 3.2.3 Características de EtherCAT

***Protocolo***

El protocolo EtherCAT esta optimizado para datos de procesos y es transportado directamente dentro de la trama Ethernet gracias a un Ethertype.
Este consiste en algunos sub-telegramas, cada uno sirviendo a un área particular de memoria de las imágenes de procesos lógicos que pueden ser de hasta 4 GBytes de tamaño. La secuencia de datos es independiente del orden físico de las terminales Ethernet en la red, el direccionamiento puede ser en cualquier orden. Comunicación por Difusión (Broadcast), Multidifusión (Multicast) y entre esclavos es posible. La trama de transferencia Direct Ethernet es usada en casos donde un máximo rendimiento es requerido y los componentes EtherCAT son operados en la misma sub-red así como el controlador.

No obstante, las aplicaciones EtherCAT no están limitadas a la sub-red: EtherCAT UDP empaca el protocolo EtherCAT en datagramas UDP/IP. Esto posibilita cualquier control con la pila del protocolo Ethernet para direccionar sistemas EtherCAT. Aun la comunicación a través de ruteadores en otras sub-redes es posible.

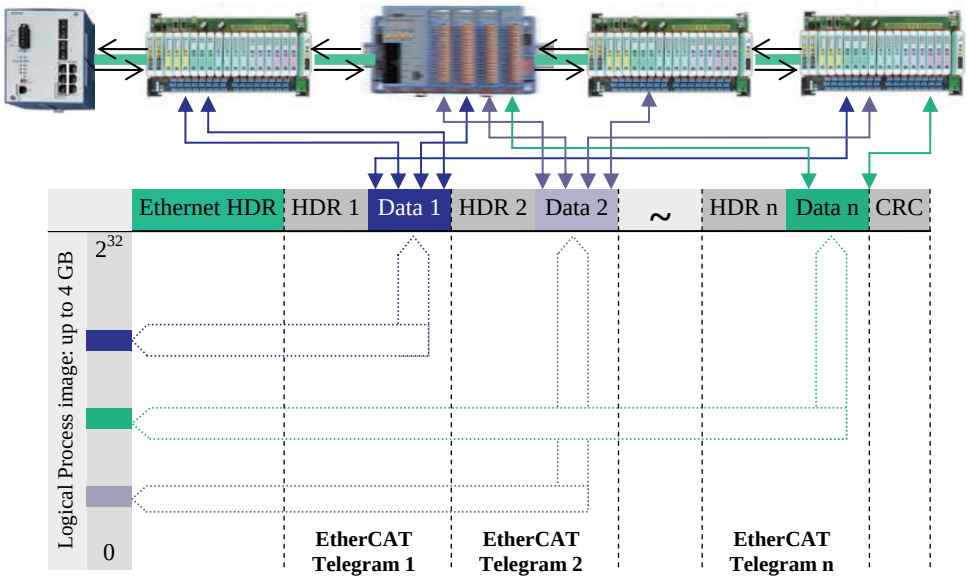



*Figura 3-11 Los datos procesados son insertados en telegramas*

En esta variante el rendimiento del sistema obviamente depende de las características de tiempo real del control y su implementación del protocolo Ethernet. Los tiempos de respuesta EtherCAT por si mismos son duramente restringidos en todo: el datagrama UDP solo tiene que ser desempaquetado en la primera estación.
EtherCAT solo usa tramas estándar – las tramas no son acortadas. Las tramas EtherCAT pueden de este modo ser enviadas por cualquier controlador Ethernet (maestro) y herramientas estándar (por ejemplo un monitor) pueden ser utilizadas.

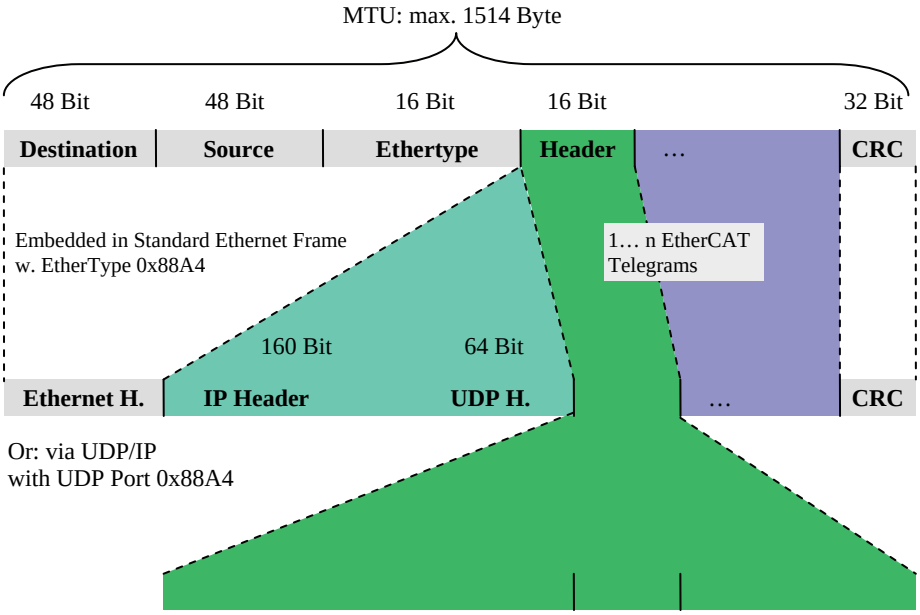



*Figura 3-12 EtherCAT: Tramas Estándar de acuerdo a IEEE 802.3*

### *Topología*

En bus, árbol o estrella: EtherCAT soporta casi cualquier topología. Particularmente útil para el sistema de cableado es la combinación de las topologías de bus y de rama o árbol. Por lo tanto se requerirá que existan por lo menos en los dispositivos 2 interfaces por cada uno y de este modo ningún switch adicional será requerido. Naturalmente, la clásica topología de estrella Ethernet basada en switch también puede ser utilizada.

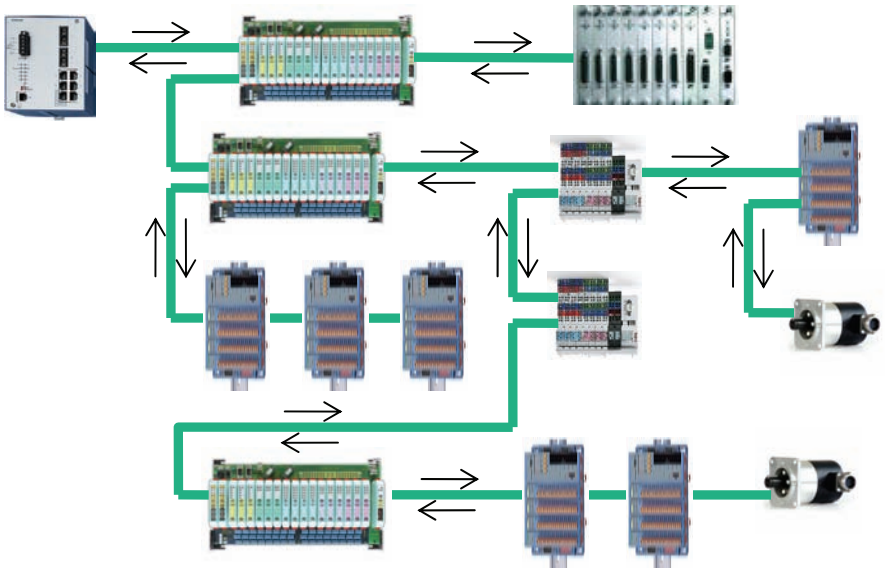


***Figura 3-13 Topología flexible: Línea, Árbol o Estrella***

La flexibilidad del cableado esta maximizada para las diferentes opciones de cables. La aplicación de EtherCAT es independiente del medio de comunicación utilizado, si este es un cable de cobre estándar para Ethernet o fibras ópticas plásticas (POF, Plastic Optical Fibres) o cualquier otro que cumpla con el estándar podrá ser usado sin problemas.

La física Fast Ethernet (100BASE-TX) posibilita el uso de un cable de 100 m entre dos dispositivos. Para cada conexión, la variación de señal puede ser seleccionada individualmente. Hasta 65535 dispositivos pueden ser conectados, así que el tamaño de la red puede ser casi ilimitado.

Dispositivos EtherCAT convertirán la comunicación Ethernet internamente en un E-Bus y el E-Bus es capaz de cubrir una distancia de 10 m más o menos y así es posible distribuir los dispositivos en un sistema EtherCAT dentro de esta distancia.

### *Relojes distribuidos*

La exactitud en la sincronización es particularmente importante en casos donde procesos distribuidos en diversos puntos requiere acciones simultáneas. Este puede ser el caso por ejemplo en aplicaciones donde algunos servos axiales llevan movimientos coordinados simultáneamente.

La propuesta más poderosa para la sincronización es como se había mencionado, en el alineamiento exacto de relojes distribuidos, como se describe en el estándar IEEE 1588. En contraste a la comunicación totalmente síncrona, donde la calidad de la sincronización sufre inmediatamente en un evento con una falla de comunicación, los relojes alineados y distribuidos tienen un alto grado de tolerancia lo que es posible debido a retrasos relacionados a fallas dentro del sistema de comunicación.

Con EtherCAT el intercambio de datos esta totalmente basado solamente en hardware de maquina. Desde que la comunicación utiliza una estructura de anillo lógica (y gracias a Fast Ethernet full-duplex también física), el reloj maestro puede determinar la compensación del retardo de propagación a los relojes esclavos individuales de manera sencilla y exacta, y viceversa.
Los relojes distribuidos son ajustados basados en este valor, lo que significa que un tiempo base muy preciso de una red con una fluctuación de significativamente menos de 1 microsegundo esta disponible. La sincronización externa, por ejemplo a través de la planta, esta entonces basado en el estándar IEEE 1588.

No obstante, la alta resolución de los relojes distribuidos no solo es usado para la sincronización, también puede proveer información exacta acerca del ritmo de la adquisición de datos. Por ejemplo, los controladores de movimiento típicamente calculan velocidades desde posiciones secuencialmente medidas. Particularmente con tiempos de muestreo muy pequeños, aun una fluctuación temporal pequeña en la posición de medición lleva a cambios largos en el paso en la velocidad computada.
Con EtherCAT la estampilla de tiempo de los tipos de datos son introducidos como una extensión lógica. El tiempo del sistema de alta resolución es unido al valor medido, lo cual es posible por el gran ancho de banda ofrecido por Ethernet. La exactitud de una velocidad de cálculo no depende de una fluctuación de la comunicación del sistema. Esto es mejor que las técnicas de medición basadas en fluctuaciones libres.

### *Rendimiento*

Gracias al hardware de integración en el esclavo y acceso de memoria directa a la tarjeta de red en el maestro, el proceso completo del protocolo toma lugar dentro del hardware y es así totalmente independiente del tiempo de procesamiento de las pilas del protocolo, rendimiento de la CPU o implementación del software.
El tiempo de actualización para 1,000 Entradas/Salidas es de solo 30 μs - incluyendo el ciclo de tiempo de E/S. Hasta 1486 bytes de datos de proceso pueden ser intercambiados con una trama sencilla Ethernet – esto es equivalente a casi 12,000 entradas y salidas digitales. La transferencia de esta cantidad de datos solo toma 300 μs.
La comunicación con 100 ejes servo solo toma 100 μs. Durante este tiempo todos los ejes son provistos con valores de comando y control de datos y estos mismos reportan su actual posición y estado. La técnica de reloj distribuido posibilita a los ejes a ser sincronizados con una desviación de menos de 1 microsegundo.

El muy alto rendimiento de la tecnología EtherCAT posibilita conceptos de control que no podrían ser realizados con sistemas de bus clásico. Con EtherCAT una tecnología de comunicación que deriva en capacidad de computo superior es combinada con las modernas PC's industriales. El bus del sistema ya no es un cuello de botella del concepto de control. E/S's distribuidas son grabadas lo mas rápido que es posible con la mayoría de las interfaces de E/S.
La principio de la tecnología EtherCAT es escalable y no se limita a la transferencia a 100 MBaud – la extensión a Gigabit Ethernet es posible.

| Datos de Proceso | Tiempo de Actualización |
|---|---|
| 256 E/S digitales distribuidas | 11 μs = 0.01 ms |
| 1000 E/S digitales distribuidas | 30 μs |
| 200 E/S análogas (16 bit) | 50 μs ↔ 20 KHz |
| 100 Servo Ejes, cada uno con 8 Bytes de datos de E/S | 100 μs |
| 1 Gateway de Fieldbus Maestro<br>(1486 Bytes de Entrada y 1486 Bytes de Datos de Salida) | 150 μs |

***Tabla 3-3 Panorama general del rendimiento EtherCAT***

### *Diagnostico*

Desde que EtherCAT usa las tramas estándar Ethernet de acuerdo a estándar IEEE 802.3, cualquier herramienta de monitoreo Ethernet puede ser utilizada para monitorear la comunicación EtherCAT. Sumado a esto, el software analizador de trafico Ethereal (una herramienta de monitoreo open source) el monitor de red Microsoft están disponibles para procesar y desplegar trafico de datos grabados EtherCAT.

Durante el nombramiento la actual configuración de los nodos (por ejemplo drives o terminales de E/S) pueden ser checadas para consistencia con la configuración especificada. La topología también debería combinarse a la configuración. Debido al reconocimiento de la topología incorporado a las terminales individuales, esta verificación no solo puede tener lugar durante el inicio del sistema, lecturas automáticas en la red son también posibles (configuration upload).

Los bits averiados durante la transferencia son detectados confiablemente a través de la evaluación del checksum CRC: el CRC de 32 bits polinomial tiene un distancia mínima de 4. Aparte de la detección y localización de un cable roto, el protocolo, la capa física y la topología del sistema EtherCAT posibilita el monitoreo individual de calidad de cada segmento de transmisión individual. La evaluación automática de los contadores de error asociados habilita la localización precisa de secciones de la red críticas. El cambio gradual de fuentes de error como son las influencias EMI (Electro-Magnetic Interferences), conectores defectuosos o cable dañado es detectado y localizado, aun si estos todavía no se forzan al limite para poner en riesgo la salud de la capacidad de la red.

### *Perfil de dispositivos*

Los perfiles de dispositivo describen los parámetros de la aplicación y el comportamiento funcional de los dispositivos incluyendo el dispositivo de clase especifico de maquinas de estado. Para muchas clases de dispositivos, la tecnología de fieldbus ya ofrece perfiles de dispositivo fiables, por ejemplo para dispositivos de E/S, drives o válvulas. Los usuarios están familiarizados con estos perfiles, los parámetros asociados y las herramientas.
Perfiles de dispositivo específicos no EtherCAT han sido por lo tanto desarrollados para esta clase de aparatos. En vez de eso, interfaces simples para perfiles de dispositivos existentes están siendo ofrecidas.

Dispositivos CANopen y perfiles de aplicación están disponibles para un amplio rango de clases de dispositivos y aplicaciones, yendo desde componentes de E/S, drives, decodificadores, válvulas proporcionales y controladores hidráulicos para la aplicación de perfiles para el proceso del plástico o maquinas textiles por ejemplo.
EtherCAT puede proveer los mismos mecanismos de comunicación que los familiares mecanismos CANopen: diccionario de objetos, PDO (Process Data Objects) – aun el manejo de la red es comparable. EtherCAT puede de este modo ser implementado con un mínimo esfuerzo en dispositivos equipados con CANopen. Grandes partes del equipo CANopen pueden ser reutilizadas.

SERCOS interface™ es conocido y apreciado alrededor del mundo como una interfaz de comunicación en tiempo real de alto rendimiento, particularmente para aplicaciones de control de movimiento. El perfile SERCOS para servo drives y la tecnología de comunicación son cubiertos por el estándar IEC 61491. Este perfil de servo drive puede ser fácilmente elaborado para EtherCAT. El canal de servicio y por lo tanto el acceso a todos los parámetros y funciones que residen en el drive, esta basado en el EtherCAT mailbox. Aquí también el foco esta en la compatibilidad con el protocolo existente (acceso a valores, atributos, nombres, unidades, etc. de los IDN's) y la expansión con respecto a la limitación del largo de los datos. Los datos de proceso con SERCOS en la forma de datos AT y MDT, son transferidos usando mecanismos de control esclavos EtherCAT. El mapeo es similar al mapeo SERCOS. La maquina de estado esclava EtherCAT puede también ser mapeada fácilmente a las fases del protocolo SERCOS.

La tecnología Ethernet de tiempo real esta por lo tanto lista y disponible para este perfil de dispositivo, el cual es particularmente amplio en aplicaciones CNC. Los beneficios del perfil de dispositivos son combinados con los beneficios ofrecidos por EtherCAT.

***Ethernet sobre EtherCAT***

La tecnología EtherCAT no solo es totalmente compatible con Ethernet, sino también caracterizada por una apertura particular "por diseño": el protocolo tolera otros servicios basados en Ethernet y protocolos en la misma red física – usualmente aun con una mínima perdida de rendimiento. No hay restricción en el tipo de dispositivo Ethernet que puede ser conectado dentro del segmento EtherCAT vía un switch. Las tramas Ethernet son pasadas a través de un túnel vía el protocolo EtherCAT, el cual es el estándar que se aproxima a aplicaciones de Internet (por ejemplo VPN, PPPoE (DSL), etc.).
La red EtherCAT es totalmente transparente para el dispositivo Ethernet y las características de tiempo real no son afectadas.

Los dispositivos EtherCAT pueden adicionalmente presentar otros protocolos Ethernet y de este modo actuar como un dispositivo Ethernet estándar. El maestro actúa como un switch Capa 2 que redirecciona las tramas a los dispositivos respectivos de acuerdo a la información de su dirección. Todas las tecnologías Internet pueden por lo tanto ser usadas en el entorno EtherCAT: Servidor Web Integrado, E-mail, Transferencia FTP, etc.

### 3.2.4 Implementación

***Maestro***

EtherCAT usa controladores Ethernet estándar donde salvar los costos reales puede ser logrado: en el maestro. La comunicación con coprocesadores no es requerida, desde que generalmente solo una trama Ethernet tiene que ser enviada por ciclo. EtherCAT por tanto es la única solución Ethernet para los requerimientos de demanda para tiempo real que no requieren tarjetas plug-in especiales para el dispositivo maestro. El controlador on-board Ethernet o una tarjeta NIC estándar de costo normal será suficiente. El maestro es generalmente implementado con solo una solución de software.

El código para muestras maestras esta disponible por un costo nominal. El software esta distribuido como código fuente y comprende todas las funciones maestras EtherCAT, incluyendo Ethernet sobre EtherCAT. Todo lo que el usuario tiene que hacer es adaptar el código, el cual ha sido creado para entornos Windows, poner el hardware que será configurado y los RTOS usados.

***Esclavo***

Un controlador esclavo EtherCAT de costo medio (ASIC o FPGA) es usado en el dispositivo esclavo. Para dispositivos sencillos no se requieren microcontroladores adicionales. Para dispositivos más complejos, el rendimiento de comunicación EtherCAT es casi independiente de la capacidad de rendimiento del controlador usado, haciendo al aparato de costo medio.

### 3.2.5 Estandarización internacional

La estandarización internacional de EtherCAT ha sido iniciada. La IEC tiene conocimiento del EtherCAT Technology Group, el cual esta a cargo de desarrollar la especificación EtherCAT, como un enlace oficial con los grupos de trabajo IEC para comunicación digital. La especificación EtherCAT fue presentada a la IEC y ya ha sido aceptada como una especificación oficial IEC (IEC-PAS).
ISO ha comenzado un procedimiento de estandarización para EtherCAT.

## 3.3 EtherNet/IP

Las arquitecturas de automatización deben proveer a los usuarios tres servicios primarios:

El primero, el control, es el más importante. Los servicios de control involucran el intercambio de datos de tiempo-critico entre dispositivos controladores como son los PLC's y dispositivos de E/S como son drives de velocidad variable, sensores y actuadores. Las redes que se dedican al envío de estos datos deben de proporcionar algún nivel de prioridad y/o capacidades de interrupción.

El segundo, las redes deben de darle al usuario capacidad de configuración para poner en marcha y mantener sus sistemas de automatización. Esta funcionalidad típicamente implica el uso de una PC o herramienta equivalente para la programación de varios dispositivos en el sistema. Esto puede ser realizado durante el servicio o durante horas de trabajo en operaciones por área de trabajo.

Finalmente, una arquitectura de red debe permitir la recaudación de datos para propósitos de desplegado en estaciones MMI, análisis y tendencia y/o detección de problemas y mantenimiento.

Las redes que pueden dar los tres servicios – control, configuración y colección de datos – entregar la mayor cantidad de flexibilidad y eficiencia para un rendimiento mas completo del sistema.
Las redes que están basadas en el modelo productor/consumidor – donde los datos son identificados, estando bastante ligados a una fuente y destino específicos – pueden soportar control, configuración y servicios de recolección de datos de una manera muy eficiente.
Las capas de aplicación usan objetos distribuidos y servicios de comunicación productor/consumidor que son apropiados para los requerimientos de las arquitecturas de automatización.
Para proveer estos servicios (*Figura 3-14*) esto no puede ser asumido como un nivel simple de red que convendrá a todos los requerimientos de aplicación como cada capa de física y de datos tienen sus propios atributos y beneficios. Donde una estructura de red multinivel es requerida la arquitectura de red debe dar consistencia a los datos entre segmentos de la red distintos.

Similarmente, donde estos servicios son provistos en una red Ethernet, no se puede asumir que otros servicios no requerirán de ese segmento de red. Los servicios productor/consumidor deben coexistir totalmente con otros servicios que pueden existir en el segmento de red (por ejemplo http para páginas web).
EtherNet/IP (con "IP" como Industrial Protocol) implementa de manera completa una suite de servicios de datos de control, configuración y adquisición de datos en una red Ethernet, y puede de este modo ser usada para los típicos niveles de información y control mostrados en la *Figura 3-14*.

### 3.3.1 Implementación CIP en Ethernet

La especificación EtherNet/IP esta disponible para su descarga desde ODVA (www.odva.org) y ControlNet International (www.controlnet.org). La especificación esta subdividida en 10 capítulos y 4 apéndices y las siguientes características están descritas en el documento:

Como se puede observar en la *Figura 3-15*, la capa de aplicación, las librerías de objetos de aplicación y los perfiles de dispositivo son consistentes entre EtherNet/IP, DeviceNet y ControlNet. Solo las 4 capas más bajas del modelo OSI de 7 capas que son dependientes de la red.
EtherNet/IP usa estas 4 capas en un camino que permite una implementación óptima de la recolección de datos, servicios de configuración y servicios de control en EtherNet/IP y que hace esto practico y seguro para usar este protocolo en el nivel de control.

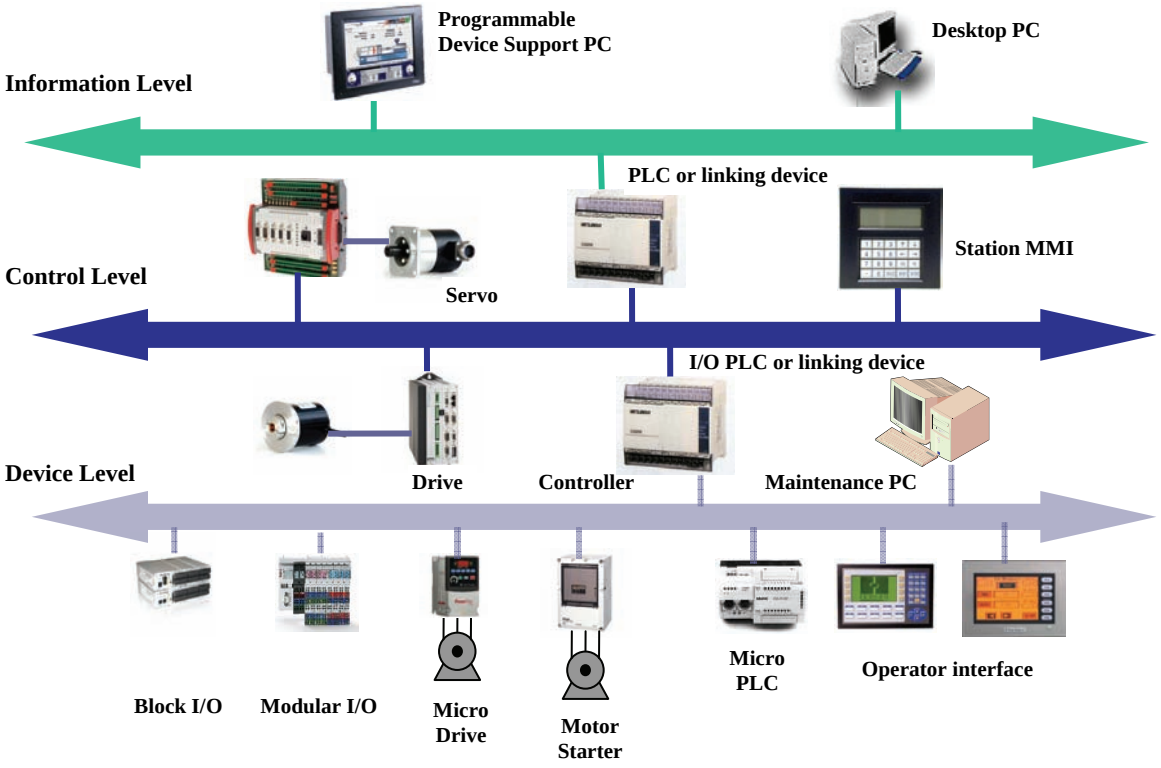



*Figura 3-14 Arquitectura típica de automatización Multinivel*

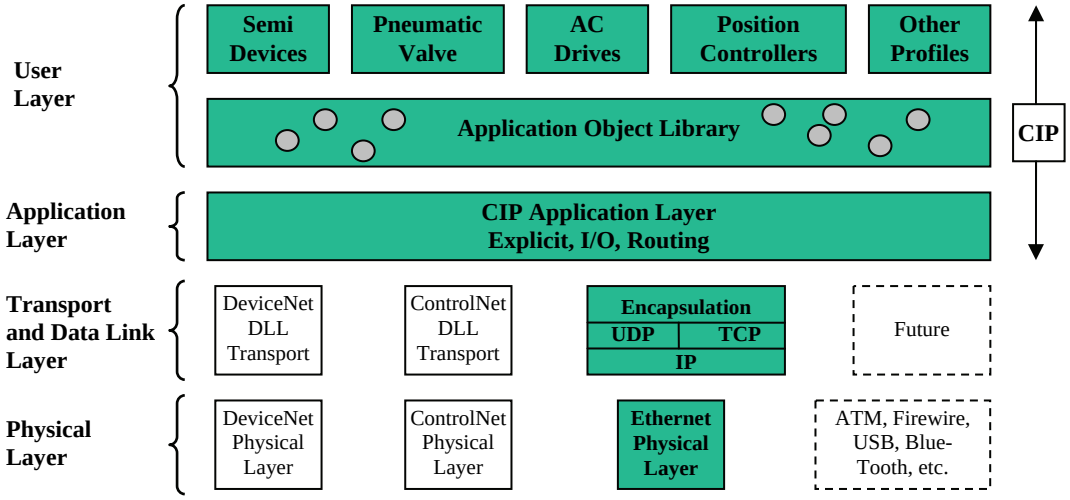



*Figura 3-15 Campo de acción de la especificación EtherNet/IP*

### 3.3.2 Coexistencia con protocolos Internet y otros

El beneficio primario que la mayoría de usuarios EtherNet/IP ganan es la influencia de entrenamiento Ethernet y conocimiento dentro de su empresa y maximizan el retorno de sus inversiones en infraestructuras Ethernet.

De manera similar ellos estarán buscando hacer el mejor y uso mas efectivo de componentes Ethernet "Commercial Off-The-Shelf" (COTS) que están disponibles hoy en día en una variedad muy grande de fabricantes que compiten entre si para bajar el costo de sus infraestructuras de red.

Estos beneficios no podrían ser realizados si EtherNet/IP requiriera una infraestructura de red personalizada (por ejemplo una infraestructura no genérica) con media física de un vendedor específico. De forma similar, ello no podría ser realizado si EtherNet/IP requiriera instalaciones de red dedicada para operar con conexión mínima o sin ella al resto de la infraestructura de red corporativa. La compatibilidad con los protocolos de Internet e intranet debe estar asegurada. Esto significa que los protocolos basados en TCP/IP serán usados en cualquier momento.

Hoy en día una instalación de una red Ethernet TCP/IP puede extenderse del plano de la planta industrial para ser conectado a una red mundial corporativa vía la Internet. Esto es generalmente usado para conducir programas de mantenimiento, envía datos a y desde sistemas MIS y MES, servir para páginas de intranet, interpretar controles de supervisión, proveer conectividad a interfaces de operador y documentar eventos y alarmas. Estas funciones requieren alta capacidad de procesamiento y accesibilidad extendida que Ethernet ofrece. En muchas aplicaciones el tiempo de respuesta es secundario para el total de la capacidad de datos. Aplicando EtherNet/IP, muchos consumidores actualmente utilizan Ethernet para propósitos de control en tiempo real, como es el control de E/S y el compartimiento de los datos del procesador (processor data sharing). En la mayoría de las aplicaciones las capacidades de tiempo real de EtherNet/IP son similares a un fieldbus de red. Para aplicaciones mas demandantes como el control de drives coordinados, extensiones del protocolo EtherNet/IP han sido creadas como son descritas en el capitulo 1.6 del manual IAONA.

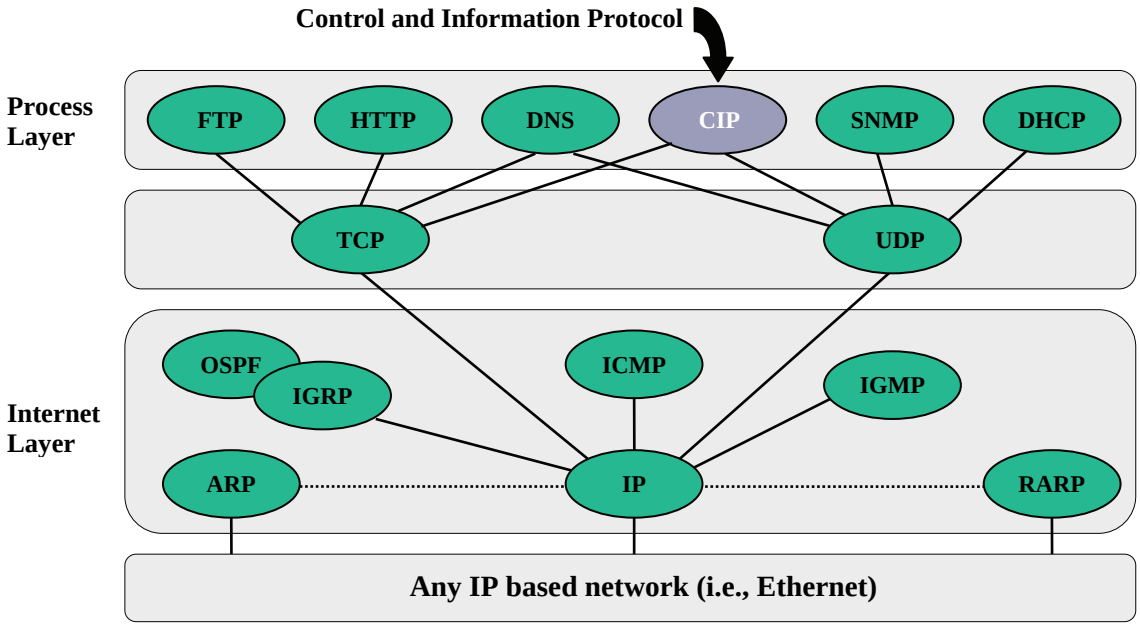



*Figura 3-16 Coexistencia de la Capa de Aplicación CIP*

### 3.3.3 El modelo del objeto CIP

Todos los datos dentro de un dispositivo CIP que están accesibles desde fuera están estructurados en objetos; el direccionamiento de estos datos es típicamente hecho a través de un método de clases, instancias o atributos.

La especificación CIP contiene una gran colección equitativa de objetos definidos comúnmente (actualmente 48 clases de objetos). Solo unas pocas clases de estos objetos (1 para DeviceNet, 3 para ControlNet y 2 para EtherNet/IP) son específicos a la red; todos los demás son objetos comunes que pueden y serán usados en todas o en las tres redes anteriores.
Cada dispositivo debe soportar un set mínimo de objetos comunes y específicos de la red. Además los objetos son sumados de acuerdo a la funcionalidad del tipo de dispositivo. Esto permite la escalabilidad de dispositivos, por ejemplo un sensor de proximidad en DeviceNet no es cargado con gastos innecesarios (burdened overhead). Un desarrollador típicamente usa objetos públicos definidos, pero también puede crear sus propios objetos en el rango específico que el vendedor quiere dar (por ejemplo Clase ID 100-199). Sin embargo esto es fuertemente fomentado para trabajar en los Grupos de Interés Especial (SIG's, Special Interest Groups) de ODVA y ControlNet Internacional para crear definiciones comunes para mas objetos en vez de inventar mas privados.
Como un ejemplo de objeto común requerido, la instancia de atributos de la identidad del objeto (Identity Object) Código de Clase: 1, son descritos en la tabla siguiente.

| **OBJETO IDENTIDAD** | |
|---|---|
| Atributos Mandatorios | Atributos Opcionales |
| ID del Vendedor | Estado |
| Tipo de dispositivo | Valor de Consistencia de Configuración |
| Código de Producto | Intervalo de Latido (Heartbeat) |
| Revisión | Lenguaje Activo |
| Status | Lista de Lenguajes Soportados |
| Numero de Serie | Nombre Internacional del Producto |
| Nombre del Producto | Semáforo |

***Tabla 3-4 Atributos de un objeto CIP***

Típicamente los dispositivos no cambian su identidad, así todos los atributos que determinan la identidad de un aparato (básicamente los atributos mandatarios) son solo leídos.

Tener un modelo de objeto consistente es una buena idea, pero los beneficios completos solo pueden ser recogidos cuando hay mecanismo de identificación para aplicaciones externas en el cual los objetos han sido implementados en un dispositivo. Esto es de particular ayuda para la configuración de dispositivos. CIP ha hecho previsiones para varias opciones en la configuración de dispositivos:

- Una hoja impresa de datos
- Parámetro de objetos y Parámetro de Objetos Finales (Parameter Object Stub)
- Hoja Electrónica de Datos (EDS, Electronic Data Sheet)
- Una combinación de un EDS y Parámetro de Objetos Finales
- Una configuración de ensamble en combinación con cualquiera de los métodos anteriores

CIP es un protocolo basado en conexión. Una conexión CIP define un mensaje que será producido en la red. Cuando una conexión es establecida, las transmisiones asociadas con esta conexión son asignadas a un Connection ID (CID). Si la conexión involucra un intercambio bidireccional, entonces dos valores de conexión ID son asignados (*Figura 3-18*).

Para permitir la creación de conexiones CIP, un proceso ha sido definido para establecer como las conexiones entre dispositivos que no están "conectados" todavía. Las conexiones son establecidas con un Mensaje Explicito de No conectado (Unconnected Explicit Message) con un servicio de apertura (Forward_Open Service) desde el nodo que origina la conexión (Connection Originator node) al nodo de conexión objetivo (Connection Target node). Este mensaje es recibido y procesado por el Unconnected Message Manager (UCMM) el cual es el responsable de procesar todos los mensajes explícitos de no conectado incluyendo peticiones de conexión. Una vez que una conexión ha sido establecida, entonces todos los recursos de comunicación necesarios en los dispositivos finales así como en cualquier router CIP intermedio están reservados.

Este método permite reducir la carga de la red y el ancho de banda requerido para el intercambio de datos.

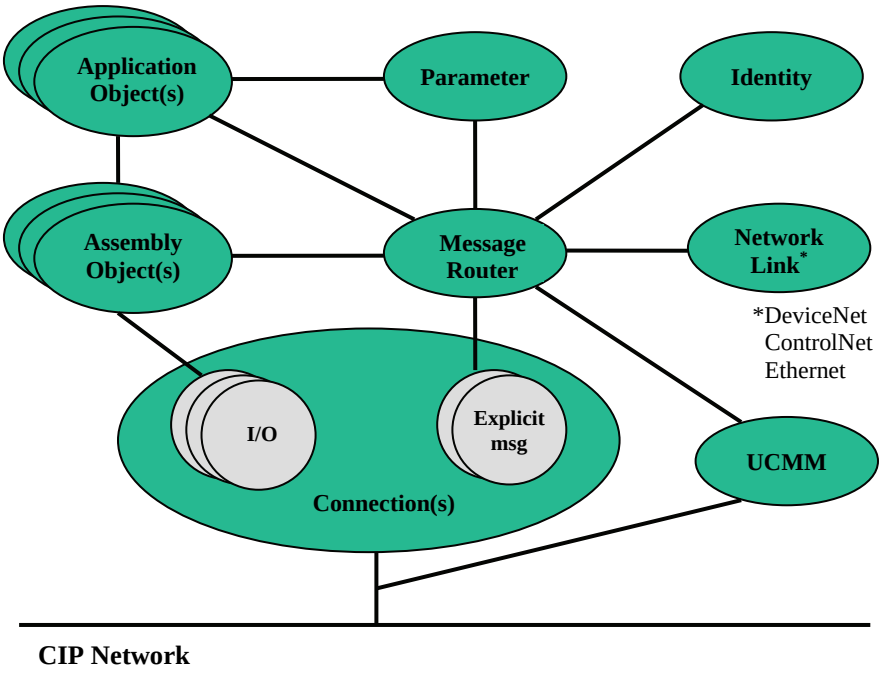



*Figura 3-17 Modelo de Objeto CIP*

Como se puede ver en el objeto modelo de la *Figura 3-17*, el acceso al modelo interno del objeto de cualquier dispositivo es encaminado o a través del Connection Object Manager o a través del Unconnected Message Manager. EtherNet/IP y ControlNet hacen uso extensivo del Unconnected Explicit Messaging a través del UCMM, mientras que DeviceNet usa la función UCMM solo para establecer conexiones.

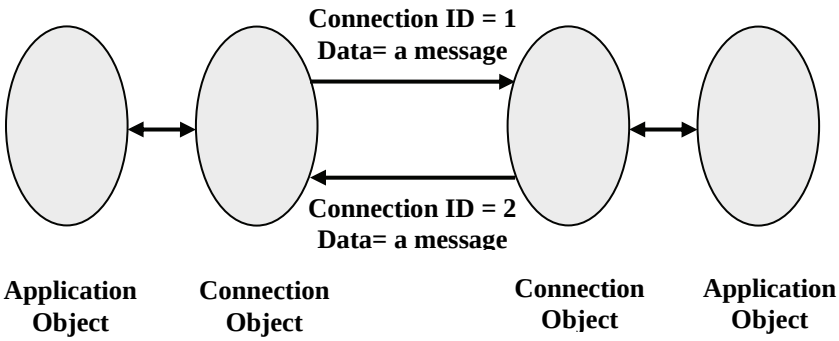



*Figura 3-18 Conexiones e Identificadores de Conexión (Connection IDs)*

Todas las conexiones en una red CIP pueden ser divididas en conexiones de mensaje explicito (Explicit Messaging Connections) y en conexiones de mensaje implícito (Implicit (o I/O) Messaging Connections).

- Las conexiones de mensaje explicito proveen trayectorias de comunicación genéricas y multi-propósito entre dos dispositivos.
- Las conexiones de mensaje implícito proveen trayectorias de comunicación dedicadas y especiales entre un objeto de aplicación productor y uno o más objetos de aplicación consumidores.

Ambos tipos de conexión pueden ser encaminados entre redes CIP y algunos detalles de conexión son discutidos con más detalle:
Como se señalo anteriormente, todas las Conexiones de Mensaje Explicito son conexiones entre dos dispositivos, los cuales requieren una dirección de origen, una dirección de destino y un ID de Conexión en cada dirección. Los mensajes explícitos son disparados por eventos externos a la capa de aplicación del protocolo CIP. Cuando los mensajes explícitos de no-conexión son ruteados a través de redes múltiples CIP, ellos también contienen información del ruteo que indica que trayectoria toma el mensaje a través de las redes CIP.

Por lo tanto, tomando la típica arquitectura de automatización en la *Figura 3-14*, un mensaje explicito de no-conexión inicia al dispositivo programable de soporte del PC conectado al nivel de información de la red y con objetivo al arranque en el nivel de dispositivo de la red contendrá dos segmentos de puerto con información que describe como el mensaje es ruteado desde el nivel información de la red en el nivel de control de la red y entonces en el nivel de dispositivos de la red.

Como discusión previa, uno de los objetos mandatorios en todos los dispositivos es el Objeto de Identidad, y atributos mandatorios de ese objeto incluyen el ID del Vendedor (ID Vendor), Tipo de dispositivo (Device Type), Código de Producto (Product Code) y Revisión. Estos datos pueden ser preguntados desde todos los nodos de una red. Desde estos datos es posible identificar únicamente los archivos EDS (EDS files) para los dispositivos y de este modo saber cuales objetos han sido hechos accesibles a través de entradas en el EDS.

Para dispositivos que contienen objetos de parámetro completos es posible conseguir estos datos directamente desde el dispositivo sin un EDS. Estos mecanismos están enfocados a la red independiente – como se puede ver en las *Figuras 3-15 y 3-17* donde los objetos son aislados de la red tal que el mismo mensaje puede ser emitido para acceder al mismo objeto no solo independientemente del dispositivo sino también independientemente de la conexión de red.

El segundo tipo de mensaje, el Mensaje Implícito, es usado cuando un intercambio de datos entre nodos esta tomando lugar entre objetos de aplicación dentro de los dispositivos, con ambos produciendo y consumiendo nodos teniendo conocimiento del contenido del mensaje antes de la transmisión.

Mientras que comúnmente son usados para el control de dispositivos de E/S, estos mensajes hacen uso total del modelo productor/consumidor y pueden ser también usados para programar comunicación entre controladores.

Estos son los 5 principales tipos de Mensajes Implícitos disponibles dentro de la especificación CIP:

- Poleo (Polled) solo en DeviceNet
- Estrobo (Strobe) solo en DeviceNet
- Poleo Multicast solo en DeviceNet
- Cambio de Estado
- Cíclico

Los mensajes cíclicos son producidos por un dispositivo en una base programada predeterminada, con un ID de conexión asociado con el mensaje. El Cambio de Estado es semejante al Cíclico excepto que (como el mismo nombre lo indica) los datos son producidos en respuesta a un evento el cual causo el cambio de los datos, en lugar de un evento predeterminado. Una conexión de cambio de estado también mantiene una tasa cíclica de fondo (heartbeat o latido) y es así como aplicaciones consumidoras pueden determinar si el nodo productor sigue trabajando bien aun si el intercambio de datos no se esta llevando a cabo. Conexiones cíclicas de E/S son las mas comunes en las redes EtherNet/IP, desde entonces ellas proveen un buen balance entre velocidad y optimización del trafico de la red.

Como se menciono arriba, las Conexiones de Mensaje son establecidas enviando un Mensaje de No-Conexión Explicito desde el Creador de Conexiones (Connection Originator) a la conexión objetivo (Connection Target).
Este mensaje contiene toda la información requerida para establecer la conexión, por ejemplo:

- ID's de Conexiones Propuestas (Proponed Connection ID's)
- Tipo de conexión (explicita o implícita)
- Mecanismos de disparo (Cíclicos, cambio de estado, disparo de aplicación, etc.)
- Tamaños de mensaje y formatos (Target → Originator and Originator → Target)
- Petición de intercambio de tasas (Requested exchange rates) (Target → Originator and Originator → Target)
- Tecleado de información (Keying information) opcional, para restringir conexiones solo a dispositivos específicos
- Información de ruteo (Routing information) solo requerida para el establecimiento de la conexión a través de múltiples redes CIP

Si el nodo objetivo es capaz de servir la petición de conexión, un mensaje exitoso se regresa al Creador de Conexión (Connection Originator) conteniendo la información requerida para correr la conexión tal como ID's de Conexión, tasas actuales de intercambio y dirección IP Multicast (si se usara).

Muchas conexiones tendrán tamaños de datos de no-cero en ambas direcciones. Las conexiones que han sido establecidas con una longitud de cero en la dirección Target → Originator u Originator → Target, usaran la longitud de conexión cero como un heartbeat para indicar que el nodo consumidor de los datos no-cero sigue activo.

Como se menciono arriba, los mensajes de E/S en EtherNet/IP pueden ser enviados en el modo uní-envío (unicast) o en un modo multi-envío (multicast). En el caso uní-envío, el mensaje es enviado vía UDP a la dirección IP de destino. Cuando un switch es usado (requerido para aplicaciones de tiempo real de EtherNet/IP), este mensaje unicast solo llegara al nodo de destino. En el caso multicast, el mensaje en enviado a una de las direcciones UDP reservadas para multicasting en el rango 239.192.0.0 a 239.195.255.255. Para notificar el nodo Creador de Conexión de la dirección IP multicast, este es incluido en la respuesta al mensaje Forward_Open que pidió la conexión.

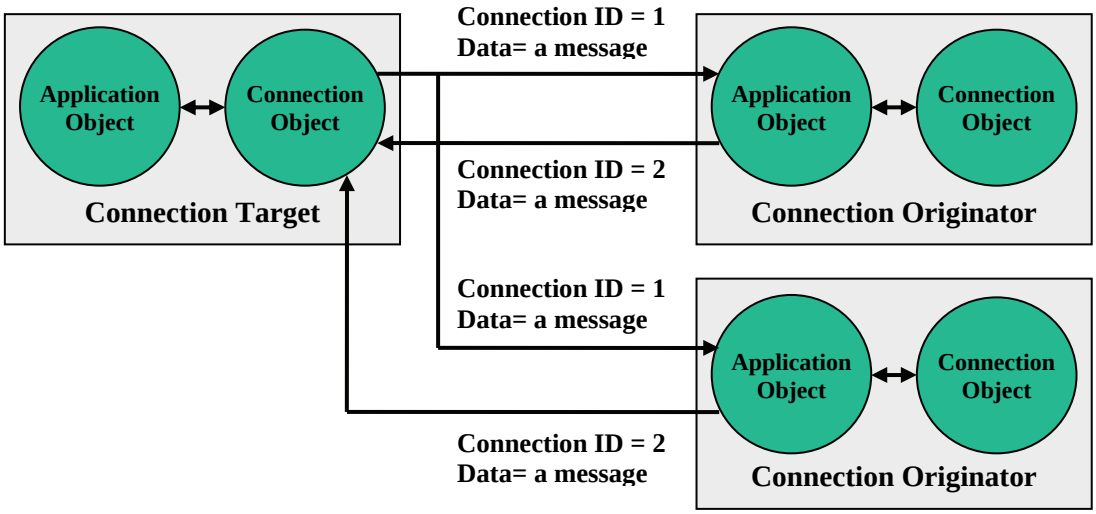



*Figura 3-19 Conexión Multicast Implícita*

Cualquier dispositivo lejano que quisiera también consumir estos datos necesita enviar otra petición Forward_Open para una conexión de “Solo Escucha” (Listen Only) de una conexión multicast al nodo objetivo. Si esa petición de conexión se ajusta a la conexión ya establecida con un Connection Originator, entonces la dirección IP multicast ya en uso es enviada al nodo que requiere la conexión “Listen Only”. Si no se encuentran coincidencias, entonces otra dirección IP multicast es asignada y el Connection Originator es notificado.

Las direcciones IP multicast son tratadas como direcciones broadcast por switches ordinarios Capa 2. Esto significa que todas las tramas multicast serán enviadas a todos los nodos en la subred aunque solo pocos nodos consuman estos mensajes. Para evitar esta “inundación” es recomendable usar switches que soporten el IGMP snooping. Con esta característica habilitada, los mensajes multicast solo se enviaran a aquellos dispositivos que han sido unidos al grupo multicast y solo a nodos que han sido notificados que las direcciones multicast harán eso.

### 3.3.4 CIP Sync y CIP Motion

Con EtherNet/IP en su forma original, las aplicaciones de tiempo real pueden ser cubiertas, pero debido al “débil” timing de link entre el Connection Originator y el Connection Target y debido a otro tráfico en la red (no CIP), una cierta cantidad del mensaje fluctuante tiene que ser aceptada en la aplicación.

Sin mayores mediciones, la fluctuación de la acción es un resultado directo de la fluctuación del mensaje en el nodo receptor, por lo tanto solo aplicaciones que pueden tolerar esta fluctuación son viables con EtherNet/IP en su forma original. Para superar esta limitación, EtherNet/IP ha sido extendido a esas aplicaciones que demandan movimiento coordinado con fluctuaciones de acción de microsegundos y se han cubierto.

Los nuevos objetos CIP han sido definidos para proveer la capacidad necesaria para alto rendimiento, operación de drives de bucle cerrado. Estas extensiones CIP están referidas como “CIP Motion”. Aunque CIP Motion por diseño es una red independiente, la implementación inicial será en EtherNet/IP. EtherNet/IP fue escogido porque tiene amplia aceptación y provee el ancho de banda requerido para bucle cerrado y control de drives distribuido.

Uno puede suponer que llevar a cabo (1) la conformidad IEEE 802.3 y TCP/IP, y (2) el uso de hardware Ethernet estándar no es posible, dado que todas las demás soluciones basadas en Ethernet, bucle cerrado y soluciones de drives distribuido han descansado en implementaciones propietarias que no cumplen completamente con el estándar IEEE 802.3.
Por el uso control de bucle cerrado innovado propone el “Control Distribuido Sincronizado en Tiempo” (Time Synchronised Distributed Control), esto es posible para usar el hardware Ethernet estándar implementando IEEE 802.3 y TCP/IP para dar alto rendimiento, el control deterministico es requerido para la operación de drives de bucle cerrado.

El control tradicional de bucle cerrado de drives distribuidos usa una sincronización basada en eventos, lo que requiere de absoluta entrega de los datos cíclicos de tiempo crítico a través de la red. Una fluctuación de <1μs para datos cíclicos es necesaria para velocidades precisas y/o control de posición. La capa de enlace de datos IEEE 802.3 CSMA/CD no es capaz de entregar datos con fluctuaciones de <1μs. Una vía para resolver esta cuestión es usando un algoritmo programado de tiempo para reemplazar la capa de enlace de datos CSMA/CD.

La implementación EtherNet/IP para aplicaciones de movimiento usa una propuesta diferente llamada “Time Synchronised Distributed Control”. Time Synchronised Distributed Control usa paquetes de tiempo sellados para relajar el estricto requerimiento de la fluctuación de <1μs para entrega de datos cíclicos.

Con esta propuesta, la capa de enlace de datos CSMA/CD no tiene que ser reemplazada con un controlador o driver propietario o ASIC, permitiendo completa conformidad con IEEE 802.3, mientras se provee una solución robusta con el rendimiento necesario para operación de bucle cerrado de drives digitales de alto rendimiento.

La tecnología usada por CIP Motion sobre EtherNet/IP incluye:

- Servicios de sincronización de tiempo (CIP Sync) IEEE 1588 con asistencia de hardware
- Telegrama de datos cíclicos sellados en tiempo (Time-stamped cyclic data telegram)
- Soporte QoS (Quality of Service) como se define en el estándar IEEE 801.2q
- Uso de switches gestionados y operación full-duplex para dar transferencia de datos libre de colisiones
- Soporte UDP/IP para transferencia de datos cíclicos
- Soporte UDP/IP para transferencia de datos acíclicos
- Soporte TCP/IP para mensajería explicita

CIP Sync define un set de servicios de tiempo que han sido adheridos a CIP los cuales son usados para enlazar la sincronización de tiempo IEEE 1588 en el modelo objeto CIP y por lo tanto EtherNet/IP.

Los servicios de tiempo proveen una referencia de tiempo distribuida por el paquete de tiempo sellado usado en el esquema del Time Synchronised Distributed Control. CIP Sync cumple totalmente con el estándar IEEE 1588 para un protocolo de sincronización de reloj preciso (Precision Clock Synchronisation Protocol) para mediciones de red (Network Measurement) y sistemas de control.

Usando el hardware en el modo asistente, los servicios 1588 proveen resoluciones de reloj de nanosegundos y sincronización de reloj de +/- 100 nanosegundos a través de controles distribuidos, drives y otros dispositivos en EtherNet/IP. Con la sincronización de tiempo es posible sincronizar operaciones a través de nodos distribuidos. La implementación CIP Sync 1588 se muestra en la *Figura 3-20*.

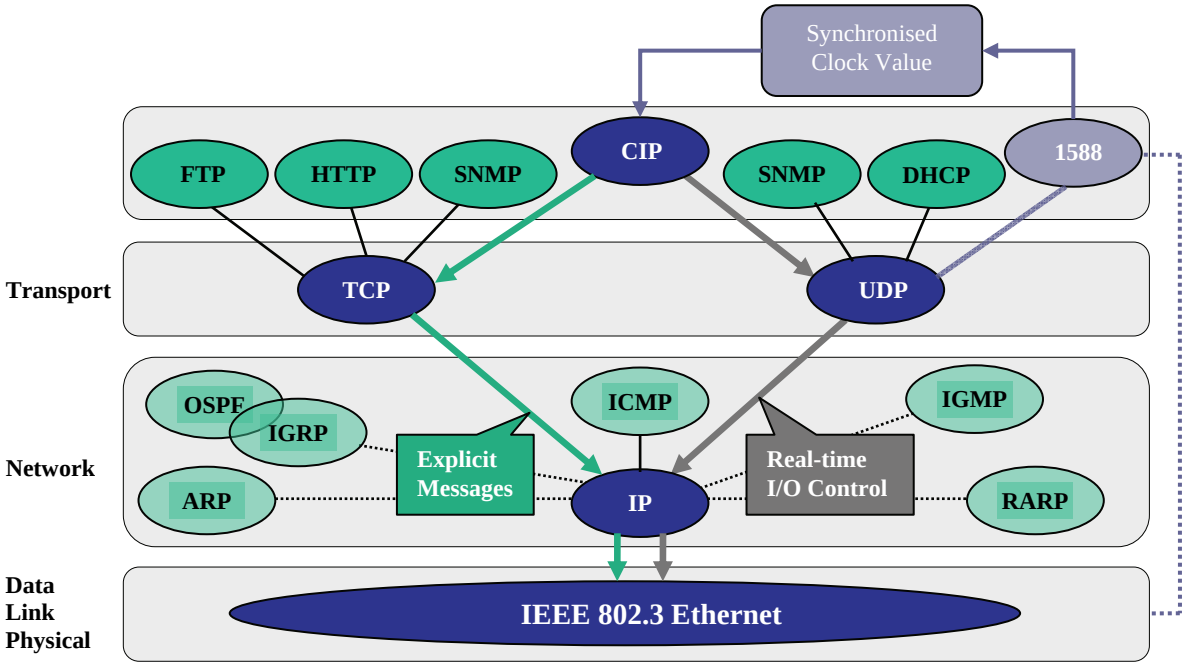



***Figura 3-20 Implementación CIP Sync – IEEE 1588***

Cuando un paquete de datos cíclicos de movimiento es construido, un sello de tiempo es incluido como parte del paquete. Un modelo de tiempo cíclico sencillo para transferencia de datos cíclicos entrega un valor de comando fresco desde el planeador de movimiento a cada drive basado en los valores actuales de posición muestreados al inicio del ciclo. Típicamente el planeador de movimiento residirá en el controlador de movimiento, con los datos repartidos a los drives distribuidos vía EtherNet/IP. Si un paquete de movimiento esta retrasado para el siguiente ciclo, el sello de tiempo del paquete puede ser usado para compensar por el retraso. Esta técnica de compensación basada en tiempo elimina la necesidad de entrega de datos absoluta, permitiendo el uso de la capa de enlace de datos IEEE 802.3 CSMA/CD, y por lo tanto eliminar la necesidad de la capa de enlace de datos propietaria requerida con otras redes de movimiento “basadas en Ethernet”.

El perfil de aplicación CIP usado en EtherNet/IP da un set completo de servicios y perfil de dispositivos que proveen un amplio rango de funcionalidad y soporte de dispositivos. CIP Motion extiende la capacidad CIP definiendo extensiones enfocadas al “drive control” como se lista a continuación:

- Torque, velocidad o control de posición de servos y VFD’s (Variable Frequency Drives)
- Configuración, status y parámetros de diagnostico para Servo y VFD drives
- Comunicaciones Unicast para control del manejo
- Comunicaciones Multicast punto-a-punto (control-to-control, drive-to-drive)
- Soporte de planeadores de movimiento centralizado y distribuido

El perfil CIP Motion esta actualmente bajo desarrollo por la ODVA Distributed Motion JSIG. Como CIP, las extensiones CIP Motion serán totalmente abiertas en conformidad y asegurando la interoperabilidad completa.

### 3.3.5 Pruebas de adaptación

La interoperabilidad es una de las principales metas de la ODVA y de ControlNet International en la generación de la especificación EtherNet/IP, esas organizaciones han puesto un cierto numero instalaciones de pruebas, una basada en Europa, una en Norteamérica y otra en Japón.
Un grupo de interés especial común (JSIG, Joint Special Interest Group) ha sido establecido entre la ODVA y ControlNet International para asegurar que pruebas y procedimientos consistentes estén realizándose en estos laboratorios.

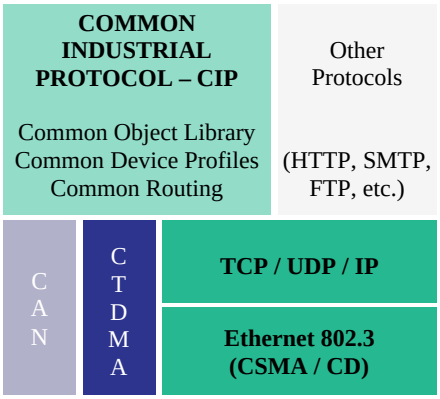



***Figura 3-21 Beneficios EtherNet/IP***

Para proveer estas facilidades, seria practico para los vendedores competitivos ofrecer productos con miedo o pérdida de la propiedad intelectual pero con la confianza de que los productos se integraran de manera uniforme. Esto asegurara que los usuarios serán capaces de tomar decisiones en base a los meritos de los componentes individuales y distribuidores con los que sientan confianza o a un solo vendedor. El primero de estos laboratorios, en la Universidad de Michigan en E.U. fue abierto el 10 de agosto del 2001. A este le fue seguida una unidad similar en la Universidad de Magdeburgo en Alemania en el 2004.

## 3.4 ETHERNET Powerlink

En la automatización industrial, la necesidad de distribuir sistemas inteligentes esta creciendo de forma continua. Sistemas distribuidos físicamente están trabajando más y mas juntos para resolver funciones comunes, las bases de datos están conectadas, los servicios y diagnósticos tienen que ser hechos por conexiones remotas, cada vez mas usando TCP/IP.

Previamente, la aplicación de diferentes sistemas de fieldbus ha dominado la planeación de acceso heterogéneo a nivel maquina, pero en el futuro Ethernet será el bus universal en la automatización.

Desde el equipamiento de oficina donde Ethernet se estableció hace 30 años como un estándar, para maquinas un sistema de bus basado en el estándar IEEE 802.3 será establecido. Recientemente esta es la tecnología dominante, en la que los usuarios tienen también profunda experiencia.
Adicionalmente, un amplio espectro de accesorios esta disponible como cable, conectores y equipamiento de calidad industrial como son hubs y switches. La necesidad de largo ciclos de vida en la industria pueden ser llenados también porque Ethernet será mejorado continuamente, justo ahora va de los 100 MBit/s a los 10 GBit/s.
La alta penetración al mercado como un estándar internacional garantiza esto también. Hoy en día es posible usar varios protocolos con Ethernet, por ejemplo TCP/IP, XML, HTTP, SNMP y muchos más. Obviamente había una necesidad de desarrollar un protocolo industrial el cual llenara los requerimientos para control en automatización como se describe en el capitulo 1 en detalle.

El principal problema fue la realización de las capacidades de tiempo real, las cuales tienen que ser garantizadas para aplicaciones de tiempo críticas, pero para conseguir transparencia en el acceso a aplicaciones y protocolos también. Se tiene que lograr una interoperabilidad real y acceso a nivel mundial en sistemas de automatización.

### 3.4.1 Un estándar abierto para comunicación en tiempo real

Ethernet regular y los bien conocidos y establecidos protocolos como TCP/IP y UDP no son capaces de transferir datos en tiempo real, fue el factor que impedía el establecimiento de Ethernet en la automatización industrial en los niveles de sensores y actuadores.

Con ETHERNET Powerlink un estándar ha sido desarrollado basado en las especificaciones IEEE 802.3. Mecanismos mezclados de poleo y cortes de tiempo arriba de las Capas 1 y 2 Ethernet permiten la transferencia de datos de tiempo crítico con ciclos de comunicación isócrona muy pequeños y precisos. Los ciclos de tiempo son configurables de una manera flexible.
Sumado a los datos de tiempo critico, el suficiente ancho de banda para transferencias adhoc de datos asíncronos para diagnósticos, parámetros y otros propósitos necesitan ser garantizados.

ETHERNET Powerlink es el único sistema Ethernet industrial de tiempo real probado en el mercado. Este esta disponible desde hace mas de tres años y ha sido exitosamente implementado en múltiples aplicaciones seriales alrededor del globo. Hoy en día los sistemas están alcanzando ciclos de tiempo por debajo de los 100 μs con un disparo de red debajo de 1 μs. De este modo ETHERNET Powerlink cubre bien las necesidades de aplicaciones demandantes en automatización.
ETHERNET Powerlink esta basado en unos estándares bien establecidos Ethernet. Por lo tanto es posible usar los componentes existentes de la infraestructura Ethernet, cualquier arquitectura de chip, equipamiento y sistemas de prueba.

Todos los protocolos basados en IP como TCP, UDP, etc. y sus aplicaciones pueden ser usados sin modificarse. En particular ETHERNET Powerlink cumple con los siguientes estándares:

- IEEE 802.3 Fast Ethernet (incluyendo formato de tramas y física)
- Protocolos IP basados en RFC 791
- Comunicación y perfil de dispositivos CANopen EN 50325-4
- Cualquier chip Ethernet en el mercado
- IEEE 1588 para sincronización de reloj en tiempo real distribuido (distributed Real-time Clock Synchronisation) en una versión futura

En suma a los estándares internacionales, ETHERNET Powerlink y partes de su tecnología por si mismas llegaran a ser un estándar. Miembros del EPSG (ETHERNET Powerlink Standardization Group) están implicados activamente en los siguientes proyectos de estandarización:

- IEC 61784-2 Ethernet de tiempo real
- IEC 61800-7 Sistemas Power Drive
- ISO 1574 Descripción de dispositivos basados en XML

### 3.4.2 Protocolos de capa más baja

La siguiente lista muestra las características básicas de ETHERNET Powerlink:

- Hasta 240 nodos en un dominio de red en tiempo real
- Comunicación deterministica garantizada
  - Tiempo real IAONA Clase 4 (de mas alto rendimiento)
  - Ciclos de tiempo menores a 100 μs implementados
  - Disparo mínimo (menos de 1 μs) para sincronización precisa
- Comunicación directa punto-a-punto de todos los nodos, por ejemplo todos los datos enviados por cualquier nodo puede inmediatamente ser leído por cualquier otro conectado a la red
- Soporte Hot-Plugging
- Integración transparente perfecta con redes IT

#### *Modelo de referencia*

La arquitectura de ETHERNET Powerlink esta estructurada de acuerdo al modelo de pilas ISO/OSI soportando los modelos de comunicación Cliente/Servidor y Editor/Suscriptor. La siguiente figura ilustra todas las capas ETHERNET Powerlink incluyendo TCP, UDP, IP y CANopen.

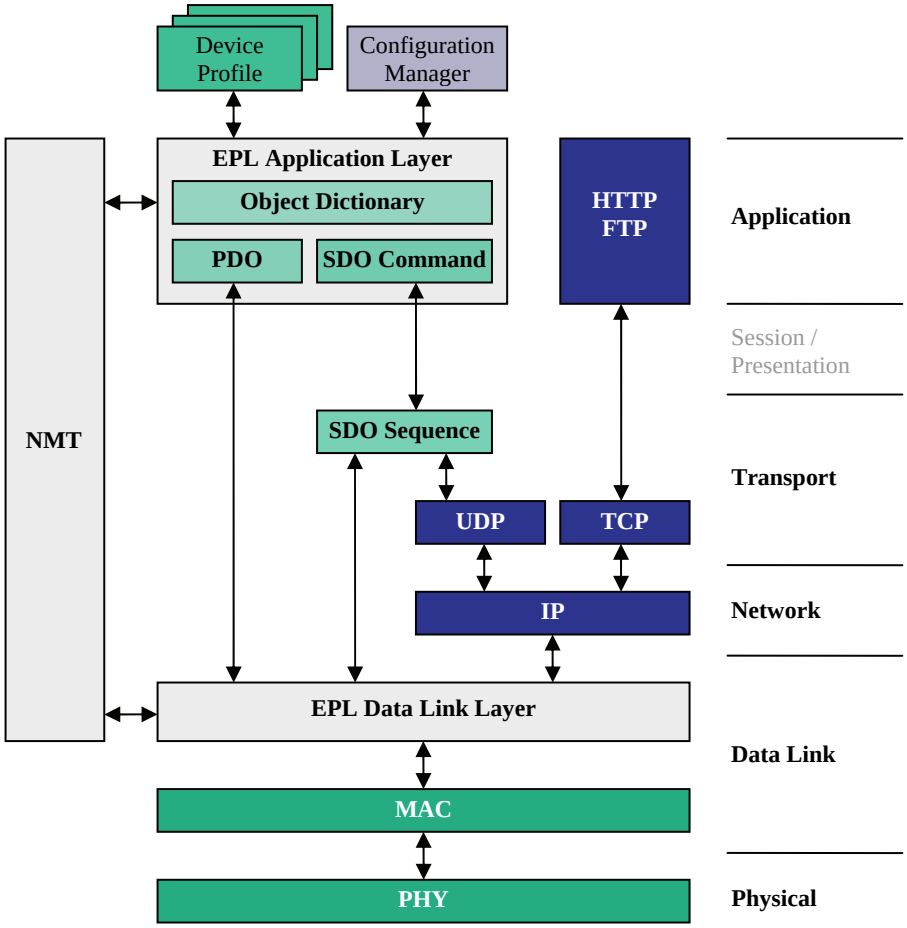



*Figura 3-22 Modelo de Referencia del protocolo Ethernet Powerlink*

### *Capa de Enlace de Datos*

Cada dispositivo ETHERNET Powerlink (EPL) soporta los siguientes modos de operación:

*1. Modo Ethernet básico*

El modo por defecto de un dispositivo EPL. Este modo permite a todos los dispositivos iniciar desde la red, recibir datos de configuración y cambiar a operación de tiempo real si se conecta a un dominio de tiempo real. Sin embargo, los nodos EPL pueden ser siempre conectados directamente a cualquier red Ethernet, no importa si es de tiempo real o no. El sistema entonces continúa en este modo y se comporta como cualquier otro dispositivo que no sea de tiempo real.

*2. Modo EPL*

El dispositivo esta corriendo con el rendimiento de tiempo real. Este se comunica con un mecanismo de división de tiempo deterministico el cual se describirá posteriormente.

***División de tiempo (Time slicing)***

Los requerimientos de tiempo real de una aplicación solo pueden ser totalmente llenados cuando esta garantiza que esa información es colectada, comunicada y procesada dentro de los límites de tiempo definidos. Las redes regulares Ethernet no son capaces de transferir datos en tiempo real. Las razones de eso son los mecanismos de acceso a la media de Ethernet (CSMA/CD – Carrier Sense Multiple Access/Collision Detect) y los retrasos (queuing delays) de los dispositivos de infraestructura como los switches. Ambos son en gran medida dependientes del trafico de red total y no permiten determinar dentro de cual tiempo de trama (timeframe) será completamente transmitida. ETHERNET Powerlink esta evitando ambos asuntos implementando un mecanismo de división de tiempo (time slicing). De este modo, se garantiza que solo un miembro del bus a un tiempo este permitido para enviar datos a la media de la red. Colisiones o retrasos por lo tanto ahora no son posibles.

Ahí se necesita al menos un nodo en el dominio de tiempo real controlando el ritmo (timing) de la comunicación. Este nodo es llamado el Nodo Director (MN, Managing Node). El MN sincroniza todos los nodos conectados y asigna tiempos de slot dedicados a cada nodo (llamados Nodos Controlados, CN – Controlled Nodes). La *Figura 3-23* da una vista previa del ciclo de comunicación EPL.

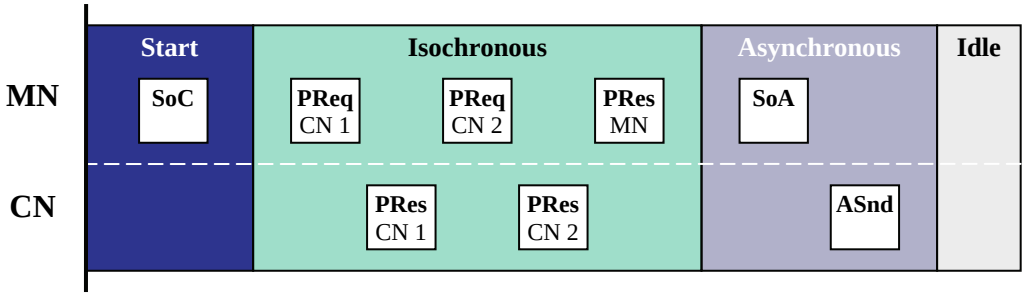



***Figura 3-23 Diagrama del ciclo Ethernet Powerlink***

El ciclo de ETHERNET Powerlink en detalle:

**1.** Un ciclo ETHERNET Powerlink siempre empieza con la fase de sincronización enviando una trama "Start of Cycle" (SoC) desde el MN. Todos los CN's sincronizan su timing con esta trama capturando y ajustando datos de E/S e inicializando el proceso de datos.

**2.** La siguiente fase es la fase isócrona en la cual los datos de tiempo crítico son intercambiados en la red. El MN esta enviando peticiones individuales a cada uno de los CN's programados.
El CN solicitado responderá con sus datos individuales los cuales serán leídos inmediatamente por todos los dispositivos conectados. Al final de la fase isócrona el MN esta enviando sus datos a todos los demás dispositivos conectados a la red.

**3.** Después de la comunicación isócrona la fase asíncrona es iniciada. En esta parte cualquier dispositivo puede enviar datos de tiempo no críticos por solicitud. En esta fase típicamente los parámetros, datos de diagnostico o archivos son transferidos. Los protocolos basados en IP pueden ser usados directamente sin conversión de datos o tunnelling.

### 3.4.3 Protocolo de Capa de Aplicación y perfiles de dispositivos

Hoy en día, los fabricantes de sistemas de automatización se están enfocando principalmente a la interoperabilidad e intercambialidad de dispositivos de varios fabricantes. Un amplio mercado de componentes con bastantes alternativas posibilita la producción de soluciones de automatización competitivas sin depender de un único o sistema propietario.

El objetivo de la independencia solo puede ser alcanzado usando soluciones estándar, las cuales proveen amplios y muy usados mecanismos de intercambio de datos. CANopen, como capa de aplicación (Capa 7) para sistemas CAN (Control Área Network), ya ha probado el poder del mercado de la estandarización con un estándar independiente de vendedor el cual da a numerosos fabricantes de dispositivos la oportunidad de participar en los sofisticados mecanismos de comunicación.

En el pasado, muchas soluciones de comunicación especificas han sido desarrolladas para la transmisión de datos planos en una Capa de Enlace de Datos (Data Link Layer) – Capa 2 – sin poner atención a definiciones adicionales de capas superiores y servicios relacionados con aplicaciones como configuración de parámetros o administración de red. La mayoría de veces, los mensajes son definidos estáticamente sin la posibilidad de modificación del contenido de los datos a ser transmitidos.
En general, hay muchos y múltiples requerimientos para un sistema de comunicación surgiendo cuando los sistemas de automatización distribuida deberán estar construidos con diferentes tipos de dispositivos o dispositivos de diferentes fabricantes:

- Administración de la red (network Management): Un mecanismo común para el controlar y monitorear la consistencia de la red durante el inicio y trabajo de la red.

- Diccionario de objetos y modelo de dispositivo: Un método común para especificar y referenciar parámetros de datos y funciones de un cierto dispositivo o tipo de dispositivo provisto al sistema.

- Señalización de errores: Un método común para señalización de errores y condiciones indicadoras de error al sistema independientes del tipo de dispositivo o fabricante.

- Objeto de Datos de Proceso (PDO, Process Data Object): Un mecanismo común que posibilita al usuario a especificar el tipo de datos intercambiados entre diferentes dispositivos.

- Objeto de Datos de Servicio (SDO, Service Data Object): Un mecanismo común para trasmitir grandes cantidades de datos arbitrarios como lo son datos de configuración.

- Perfiles de dispositivo (Device Profiles): Definiciones estandarizadas de datos, parámetros y funciones para cierto tipo de dispositivos como drives, módulos de E/S, encoders, PLC's, etc.

***La perfecta combinación: CANopen y ETHERNET Powerlink***

Con objeto de dar una flexible y probada solución para la capa de aplicación, ETHERNET Powerlink ha sido combinado con la bien conocida y ampliamente desarrollada familia de comunicación y perfiles de dispositivos CANopen. El EPSG y la CiA (CAN in Automation) ha fundado y unido a un grupo técnico de trabajo, el cual ha conseguido la adaptación de los perfiles CANopen DS301 y DS302 a ETHERNET Powerlink.

Ahora cada dispositivo ETHERNET Powerlink esta descrito por un Modelo de Dispositivo estandarizado con su elemento central, el Diccionario Objeto (Object Dictionary) conteniendo una lista de descripciones de todos los datos, parámetros y funciones del dispositivo que pueden ser accedidos o controlados remotamente vía Ethernet. Además todos los parámetros configurables de comunicación están listados en el Diccionario Objeto. Esto significa al Diccionario Objeto que cada dato de un dispositivo puede ser fácilmente consultado por cualquier dispositivo de la red por una única referencia de 24 bits, que consiste de un índice de 16 bits y un sub-índice de 8 bits.

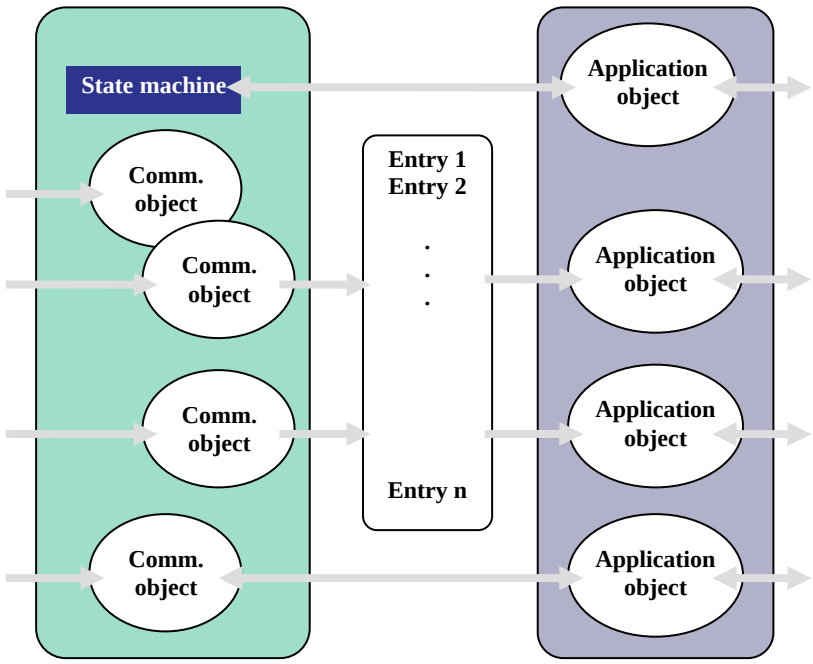



***Figura 3-24 El Modelo de dispositivo Ethernet Powerlink Device coincide con la especificación CANopen***

### *PDO's y SDO's*

El intercambio de datos de proceso críticos en tiempo real es manejado por Objetos de Datos de Proceso (PDO's). Los PDO's son transmitidos en la fase isócrona del ciclo ETHERNET Powerlink usando un modelo de comunicación Productor/Consumidor orientado. Cada dispositivo es capaz de comunicar sus datos de proceso directamente con todos los demás dispositivos en el sistema.
El contenido de un PDO (datos de proceso los cuales son transmitidos o recibidos) puede ser configurado durante el inicio del sistema. Esto permite optimizar y ajustar el intercambio de datos en Tiempo-Real a los requerimientos de la aplicación. Los datos críticos de Tiempo-Real son transmitidos en los PDO's sin ninguna cabecera (overhead).

| Ethernet Header 14 | EPL Header 6 | PDO Version 1 | res 1 | Size 2 | PDO-Objects 0 … 1490 | Ethernet CRC 4 |
|---|---|---|---|---|---|---|

***Figura 3-25 Formato de trama EPL para transferencia PDO***

El intercambio de parámetros, funciones o menos datos críticos de Tiempo-Real son manejados por los Objetos de Datos de Servicio (SDO's). Los SDO's están basados en un modelo de comunicación Cliente/Servidor orientado, donde cada dispositivo puede acceder o puede ser accedido por cualquier otro dispositivo vía un SDO. Un SDO permite un cliente para implícitamente direccionar cualquier entrada en el Diccionario Objeto del servidor. La longitud de los datos a ser transferidos no tiene límite.

Desde que los SDO's son transmitidos en la fase asíncrona usando UDP/IP, un dispositivo ETHERNET Powerlink puede también ser accedido vía Internet genérico el cual es conectado vía un router con el segmento ETHERNET Powerlink.

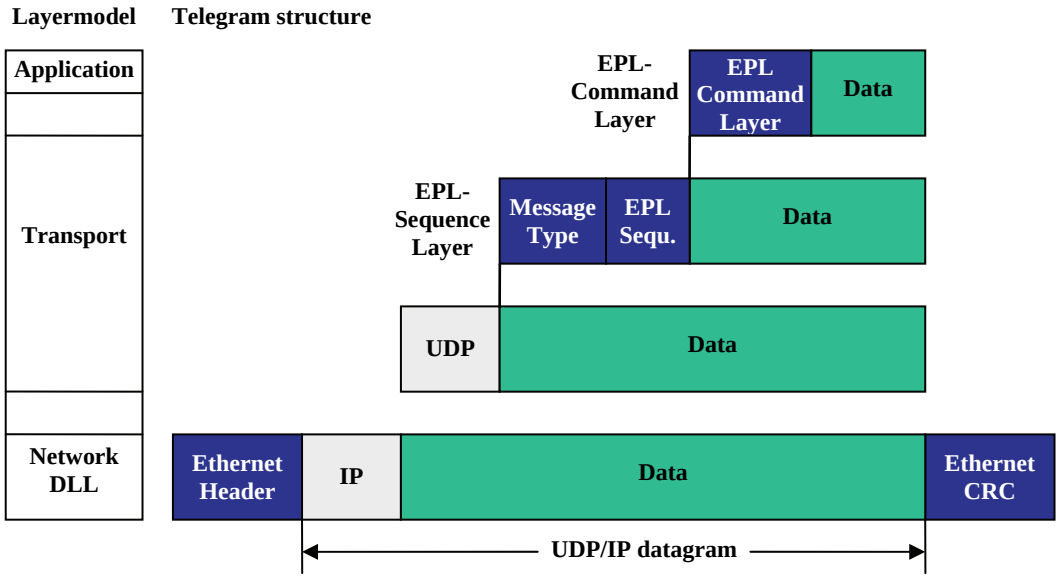



*Figura 3-26 Transferencia SDO vía UDP/IP*

### *Administración de la red*

El inicio o el apagado del sistema así como el reemplazo de dispositivos tienen que seguir reglas específicas y por lo tanto tiene que estar completamente bajo control. Funciones específicas y mecanismos tienen que ser provistos por la administración de la red. Un administrador de la red es el responsable de la consistencia del chequeo del sistema durante el inicio y del monitoreo del estado de todos los dispositivos durante el tiempo de trabajo (run-time). El comportamiento de cada dispositivo ETHERNET Powerlink esta definido por una maquina de estado local, la cual es controlada por ciertos eventos del sistema y por comandos enviados por el administrador de la red.

### *Administración de la configuración*

El administrador de la configuración es la inteligencia central en un sistema ETHERNET Powerlink. Este es capaz de mantener los datos de configuración para sus aplicaciones y todos los dispositivos locamente y descargar los datos de configuración durante el inicio del sistema.
Este enfoque posibilita poner en marcha (set-up) y conectar y usar (plug & play) sistemas los cuales permiten instalación inicial y reemplazo de dispositivos con fallas muy fácilmente.
Para describir un dispositivo ETHERNET Powerlink, un formato de archivos estandarizado existe en forma de una Hoja Electrónica de Datos (EDS, Electronic Data Sheet) basada en XML de acuerdo a la norma ISO-15745-4.

### *Integración y migración de la red*

Ya que la Capa de Aplicación de ETHERNET Powerlink proporciona los mismos mecanismos que CANopen, todos los perfiles de dispositivos CAN pueden ser directamente reutilizados. De este modo existe un amplio rango de perfiles para diferentes tipos de aparatos y aplicaciones.

Los usuarios y vendedores de dispositivos CANopen son capaces de migrar fácilmente sus aplicaciones desde un bien establecido bus CAN a un entorno Ethernet el cual es cientos de veces mas rápido que dicho bus y redes Ethernet que pueden ser combinadas de forma transparente donde sea necesario.

### 3.4.4 Integración IT

La idea de integración IT y redes de automatización usando Ethernet ofrece interoperabilidad, flexibilidad y acceso transparente al mundo a través de Internet. Con ETHERNET Powerlink una comunicación perfecta con sensores y actuadores es alcanzada usando protocolos basados en IP en dominios de tiempo-real y no-real.

#### *Asignación de direcciones IP sencillas*

Si dispositivos individuales son contactados usando una dirección IP a nivel maquina, es importante que cualquier dispositivo de reemplazo tenga la misma dirección IP de nuevo.
Con ETHERNET Powerlink, la dirección del dispositivo esta ligada con el switch de selección de nodo que esta al frente de de cada dispositivo. Este método es usado para calcular la dirección IP por si mismo, pero esta se puede seguir reescribiendo por un administrador si fuera necesario.
Esto garantiza que los dispositivos que son intercambiados guarden su dirección IP sin que estas tengan que ser ingresadas manualmente.

#### *Acceso transparente a nivel mundial*

Debido a que el número de direcciones IP disponibles en el mundo es limitado, es usualmente el departamento IT de una compañía el que se encarga de asignarlas a los dispositivos. Si los dispositivos de automatización como PLC's o drives deben ser accedidos vía redes IT abiertas, las direcciones IP necesitan ser asignadas a estas. Aparentemente, en la producción en serie el número de dirección IP necesitadas pueden alcanzar grandes números.
Sumado a esto, los rangos de direcciones IP están variando porque el fabricante y el entorno de red del usuario son distintos.

ETHERNET Powerlink se da con direcciones IP locales asignadas (RFC 1918 – Asignación de direcciones para redes privadas) a nivel maquina, a pesar de que la maquina este conectada a la red de producción del vendedor o al sitio final del consumidor. Las misma direcciones locales son siempre usadas en la maquina.

El NAT (Network Address Translation) es usado para asignar direcciones globales a direcciones locales internas en la red donde la maquina esta funcionando. Este método ha sido bien establecido en el entorno Internet. Con ETHERNET Powerlink, esto es usado para claramente separar las direcciones de fabricante y usuario final sin un proceso de reconfiguración largo después de la entrega.

Para direcciones EPL privadas Clase C la dirección 192.168.100.0 es usada. Las redes Clase C soportan 254 direcciones IP, las cuales armonizan con el nodo ID en la red EPL (192.168.100.NodeID).
Para la mascara de subred EPL por defecto es 255.255.255.0 con un gateway por default con dirección 192.168.100.254.

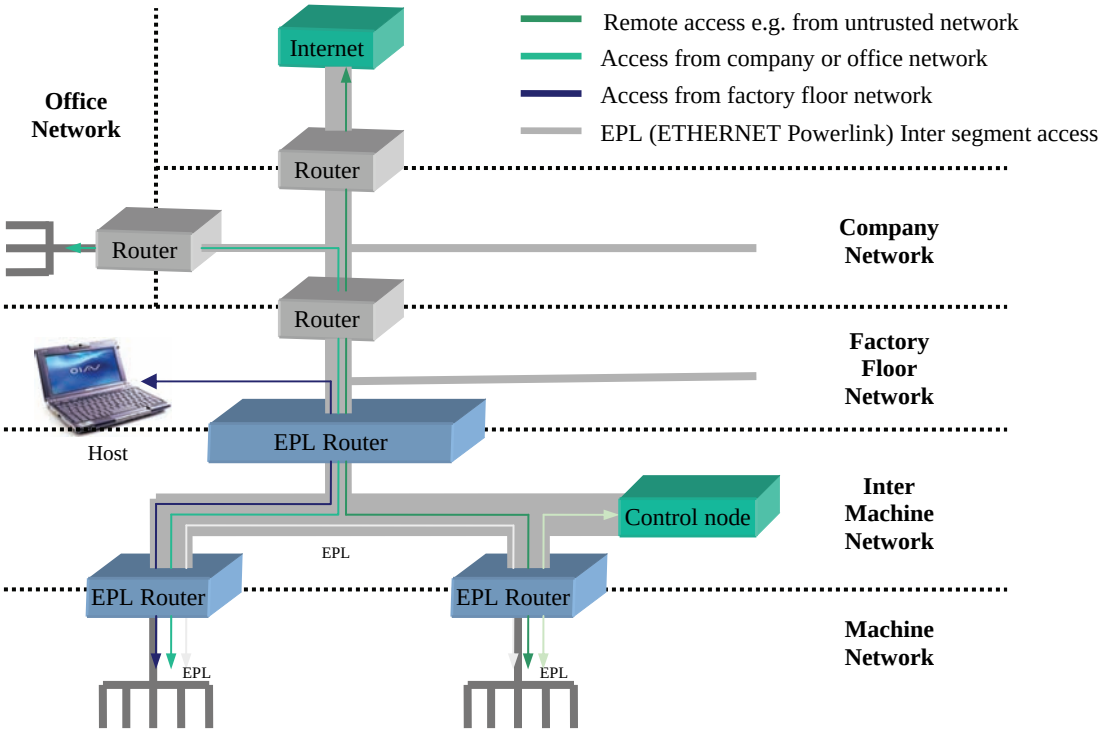



***Figura 3-27 Relaciones de comunicación típicas y trayectorias de ruteo entre las redes de Internet, de compañías, de fábricas y de redes de maquinaria***

### 3.4.5 Topologías de red

Las redes Ethernet instaladas en edificios de oficina tienen en su mayoría topología en estrella. Esto no es adecuado para la mayoría de redes de maquinaria. Los buses de campo ayudan a reducir el esfuerzo del cableado mientras adaptan la topología de la red a las necesidades de la aplicación. Ethernet industrial ayuda a tener éxito en el nivel mas bajo usando cualquier topología de red. Es por esto que los dispositivos individuales ETHERNET Powerlink están equipados con varios puertos Ethernet los cuales pueden manejar líneas y extensiones. Por lo tanto cualquier topología como línea o bus, árbol, estrella o combinada pueden ser realizadas. Dentro del dispositivo, un hub repetidor reenvía el flujo de datos a la dirección deseada. En adición a esta gran flexibilidad se reduce la necesidad de componentes de infraestructura externos como switches o hubs repetidores.
Con ETHERNET Powerlink la topología física y lógica de la red están separadas. Es posible conectar un dispositivo a cualquier puerto en la red sin tener que reconfigurar éste. Esto consigue un alto grado de libertad cuando se diseña y se actualizan los sistemas modulares de maquinas y previene errores en el cableado.

Esto es muy simple para integrar ETHERNET Powerlink con redes basadas en Ethernet en la fábrica y en la Internet. No obstante, una red de tiempo real tiene que ser protegida de fallos externos y acceso no autorizado. Además se garantiza el comportamiento en tiempo real y la precisión en el dominio del tiempo real regular del trafico basado en IP necesita ser capaz de fluir a través de la red de forma transparente si esta direccionada al dominio del tiempo real. Un router separa el dominio de tiempo real de las otras redes.

ETHERNET Powerlink distingue entre dominios de tiempo-real y dominios de no-tiempo-real. Esta separación iguala los conceptos típicos de maquina y planta. Esto también satisface el incremento de demandas de seguridad para prevenir ataques de hackers a nivel maquina o dañar a través de comunicaciones de datos erróneas en las jerarquías de red mas altas. Los grandes requerimientos de tiempo-real son apropiados dentro del dominio de tiempo-real.

Menos datos de tiempo critico son ruteados transparentemente entre el dominio de tiempo-real y el dominio de tiempo-no-real usando tramas IP estándar. Un claro limite entre una maquina y la red de la fabrica previene flujos potenciales de seguridad desde el comienzo mientras se mantiene la transparencia completa de los datos.

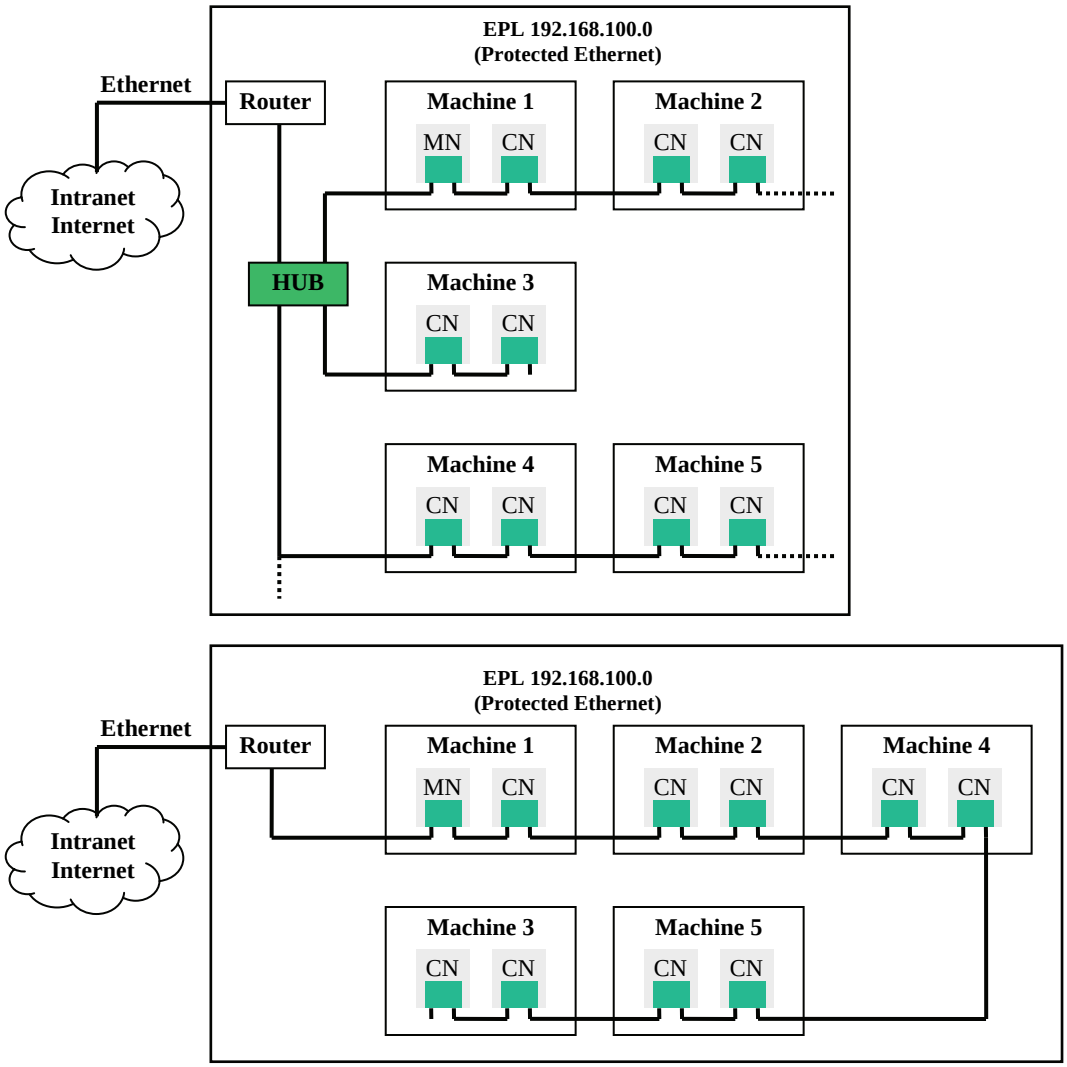



*Figura 3-28 Independencia entre la topología física y la topología lógica*

### 3.4.6 Conectado al mundo de manera segura

Una de las mayores razones para usar Ethernet industrial es la transparencia alcanzada cuando los datos transferidos a aplicaciones estándar como bases de datos, sistemas de control de procesos, sistemas ERP, etc. La accesibilidad del sistema sobre la Internet también ofrece nuevas posibilidades para mantenimiento y servicio.
Los hackers, cansados de solo romper sistemas de e-mail, están esperando el tiempo en el que un gran numero de maquinas estén conectadas en redes globales. El potencial de pérdida debido a paros en la producción, reducción de calidad o daño general es enorme.
Por esta razón, ETHERNET Powerlink provee una clara separación y controles de acceso a nivel maquinaria desde el inicio. Por el otro lado, es necesario garantizar que acceso externo a la red de maquinaria sea solo posible por personas autorizadas.

Además es importante garantizar que el dominio de tiempo-real no este influenciado por ataques maliciosos en la red de mayor nivel. Desviaciones de tiempo en el rango de microsegundos podrían causar reducción de la calidad de producción y en el peor caso, podría también dañar partes de la maquinaria. La separación entre los dominios de tiempo-real y no-real en ETHERNET Powerlink afirma la seguridad en todos los aspectos.

### 3.4.7 Seguridad ETHERNET Powerlink

Hoy en día la maquinaria, las plantas y los sistemas de seguridad están ligados a un esquema rígido hecho de funciones de seguridad basadas en hardware. Las consecuencias de esto son el costo del cableado intensivo y las opciones de diagnostico limitadas. Los intentos mas recientes con seguridad de buses de campo están caracterizados por estándares propietarios y tiempos de ciclo limitados en el rango de los milisegundos. Estos buses serán obsoletos debido al rápido desarrollo de Ethernet Industrial de Tiempo-Real.

Un meticuloso análisis de los protocolos seguros existentes ha mostrado que estos no son adecuados para ser integrados dentro de una red Ethernet abierta de tiempo-real. Por lo tanto el EPSG ha definido la siguiente generación de protocolos seguros para Ethernet Industrial: ETHERNET Powerlink Safety (EPLsafety). EPLsafety permite la comunicación Editor/Suscriptor y Cliente/Servidor.
Los datos seguros relevantes son transmitidos vía una trama de datos incrustada dentro de mensajes de comunicación estándar. Medidas para evitar cualquier falla no detectada debido a errores sistemáticos o estocásticos son una parte integral del protocolo seguro. EPLsafety se ajusta a la norma IEC 61508. El protocolo llena los requerimientos SIL 3, y dentro de arquitecturas especificas también el SIL 4. Las técnicas de detección de errores no tienen impacto en las capas de transporte existentes.

#### *Formato de trama EPLsafety*

La trama de datos relacionada a la seguridad permite transferir datos con una capacidad de 0 a 32 bytes. Usando una estructura específica cualquier falla sistemática o estocástica puede ser detectada. La probabilidad de error residual es menor de $8x10^{-21}$ por trama y en transmisión punto-a-punto una falla de un bit esta en el rango de 1 en $10^{-3}$.

Propiedades de trama:

- Un tipo de trama para todos los datos
- CRC dinámico dependiendo del largo de los datos de carga
- Alta inmunidad contra fallas estocásticas de bit
- Implementación simple con hardware dual microcontrolador
- Formato de trama EPLsafety flexible

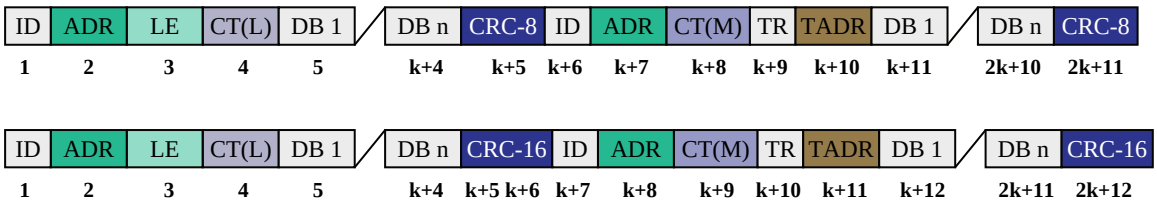



***Figura 3-29 El formato de trama EPLsafety permite máxima flexibilidad para transferir datos relacionados a la seguridad***

***Mecanismos de detección de errores***

Para poder evitar fallos e incrementar la disponibilidad de una trama valida tiene que ser distinguido de otras tramas las cuales contienen datos inválidos o están retrasados. La validez de los datos puede ser checada con CRC's. El retraso puede ser checado por comparación del tiempo de cada trama desde el productor, el tiempo local en el consumidor y la diferencia de tiempo entre el productor y el consumidor. Esto es calculado por el mecanismo de sincronización de tiempo.

## 3.5 Modbus/TCP

**Introducción**

Modbus/TCP puede ser visto como uno de los exploradores de la comunicación Ethernet a nivel industrial. Este es el protocolo con más nodos instalados a nivel mundial. Usando Modbus/TCP entre controles, PC's industriales, interfaces hombre-maquina (HMI), drives y otros los datos entre estos pueden ser intercambiados. Además, este protocolo es una alternativa seria que fue diseñada para sistemas convencionales de fieldbus. Por ejemplo, la velocidad de intercambio de datos de E/S es superior a los sistemas de fieldbus – tiempo- real en el sensado discreto y de automatización de procesos de este modo pueden ser llevados a cabo bajo ciertas circunstancias. Además, Modbus/TCP ofrece la posibilidad de intercambiar bloques enormes de datos con dispositivos los cuales sean configurados como de E/S – otra ventaja en comparación a sistemas de fieldbus convencionales. Debido a los tiempos extremadamente pequeños en los que corren los telegramas en Ethernet a 100 Mbit/s los tiempos correspondientes de reacción están grandemente influenciados por el largo de estos bloques de datos.

### 3.5.1 Estándares abiertos

Sin duda Ethernet TCP/IP puede ser denominado como el "pilar soporte" de la tecnología de comunicación tanto en la oficina como en la automatización industrial. Desde la Capa 1 a la Capa 4 del modelo de referencia ISO/OSI este representa el centro sólido de la comunicación; la única pregunta sin contestar es la de la interacción de dispositivos de automatización en la Capa de Aplicación 7 del modelo de referencia ISO/OSI. Como estándar industrial por omisión Modbus/TCP ofrece una buena forma de acercarse aquí: el protocolo es soportado y mejorado por la organización Modbus-IDA.

Modbus/TCP es fácil de manejar por el usuario y posibilita una comunicación eficiente – desde mensajes punto a punto a escaneo completo de E/S. un creciente numero de fabricantes de dispositivos aprecia la implementación fácil y rápida así como la escalabilidad del protocolo el cual ofrece la posibilidad de implementar solo aquellas partes de la especificación las cuales son realmente necesarias para la aplicación.

### 3.5.2 Modbus/TCP en su camino al estándar IEC

En Septiembre del 2004 Modbus/TCP fue aceptado y llamado "Especificación Públicamente Disponible, (PAS, Publicly Available Specification)" (IEC PAS 62030 / pre-estándar) por la IEC. Por esto Modbus/TCP es una de las vías de un estándar industrial por omisión a un estándar IEC reconocido a nivel mundial.

### 3.5.3 Detrás de la escena en Modbus/TCP

Modbus/TCP es un protocolo Cliente/Servidor: el servidor procesa una petición del cliente y consecuentemente responde esta petición – posiblemente acompañada por los resultados respectivos o un correspondiente mensaje de error conteniendo información acerca de la fuente del error. Para el usuario el procesamiento de cómo una petición sucede es de forma absolutamente transparente en el fondo (background). En implementaciones usuales no es necesario un programa de aplicación del lado del cliente. La *Figura 3-30* describe la estructura de la pila del protocolo Modbus/TCP, mapeado al modelo ISO/OSI. Además, todas las especificaciones y estándares de las capas sencillas se explican a continuación.

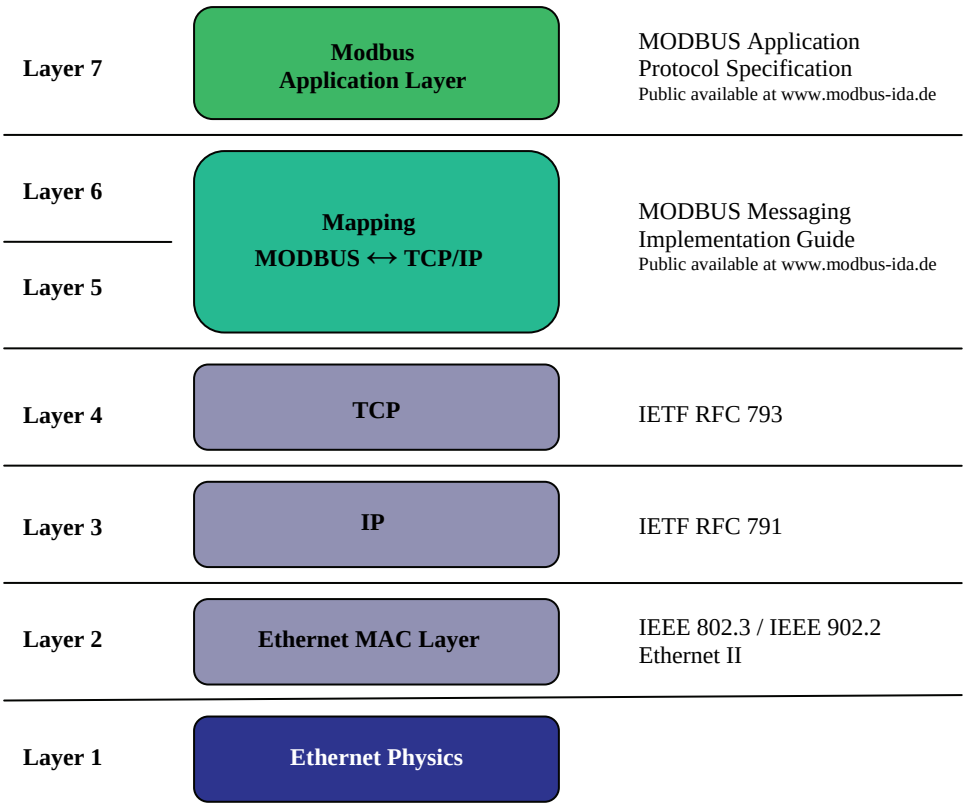



***Figura 3-30 La pila del protocolo Modbus Mapeada al Modelo de Referencia ISO/OSI***

La estructura principal de una trama Modbus/TCP se muestra en la *Figura 3-31*. Al largo del telegrama Modbus se le agregan momentáneamente 249 bytes. Esto siempre empieza – independientemente de si es una petición o una respuesta – con un código de función (largo: 1 byte), el cual depende de la composición adicional del siguiente arreglo de datos. La implementación de un checksum CRC fue desatendida en Modbus/TCP y este esta garantizado en la Capa 4 del protocolo TCP.
A los datos los cuales son transmitidos por Modbus/TCP se les permite contener información en forma de bits y en forma de palabras. Esto no dice nada acerca de la organización interna de los dispositivos a estos datos. Un productor de dispositivos puede – dependiendo de la funcionalidad – ordenar para absolutamente separadas, respectivamente áreas de memoria superpuestas en este contexto.
La información que es mas larga que 1 byte (por ejemplo, una palabra de 16 bits) esta escrita en el telegrama Modbus de modo que los bytes mas altos son enviados primero. Las cadenas de bits del bit más alto se envían primero.

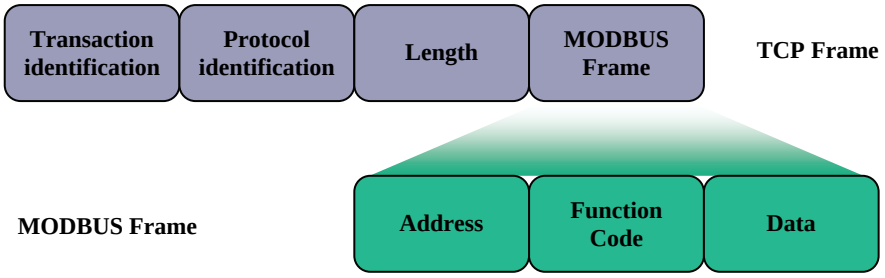



*Figura 3-31 Estructura general de una trama Modbus/TCP*

| Area Interna de Almacenamiento | Tipo de Objeto | Tipo de Acceso | Observación |
|---|---|---|---|
| Entradas | Bits sencillos | Solo lectura | Datos resultado del estado de entrada del dispositivo |
| Bits Internos (Rollos) | Bits sencillos | Lectura/Escritura | Información de Bits variable por aplicación |
| Registro de entrada | Palabra 16 Bit | Solo lectura | Datos resultado del estado de entrada del dispositivo |
| Registro Interno | Palabra 16 Bit | Lectura/Escritura | Palabras Internas variables cambiables por aplicación |

*Tabla 3-5 Tipos de Datos Modbus*

La forma de acceder a los datos de los dispositivos es manejándolos vía los mencionados códigos de función. En este contexto uno diferencía entre códigos de función públicos y definidos por el usuario. Los códigos de función públicos (códigos 1 al 64, 73 al 99 y 111 al 255) están arreglados y bien definidos (por ejemplo como parte del RFC Modbus, status: inicial, presentados al IETF (Internet Engineering Task Force). Además, para este tipo de código la posibilidad de un test de conformidad existe, por lo cual los productores son capaces de tener probada y certificada la conformidad con la especificación.

En contraste, los códigos de función definidos por el usuario (códigos 65 al 72 y 100 al 110) están diseñados por el propio productor y de este modo la necesidad no necesariamente será distinta. Una visión general de los códigos de función públicos se muestra en la *Tabla 3-6*.

| | | | | FUNCTION CODE | | |
|---|---|---|---|---|---|---|
| | | | | Code | Subcode | (Hex) |
| Data access | Bit Access | Input bits | Read input bits | 02 | | 02 |
| | | Internal bits | Read internal bits | 01 | | 01 |
| | | | Write internal bit | 05 | | 05 |
| | | | Write internal bit chain | 15 | | 0F |
| | Word access (Register) | Input word | Read register | 04 | | |
| | | Internal word | Read word table | 03 | | |
| | | | Write register | 06 | | |
| | | | Write word table | 16 | | 10 |
| | | | Sync. read/write of tables | 23 | | 17 |
| | | | Flag register | 22 | | 16 |
| | Data set | | Read data set | 20 | 6 | 14 |
| | | | Write data set | 21 | 6 | 15 |
| Interface | | | Read device identification | 43 | 14 | 2B |

*Tabla 3-6: Códigos de Función Públicos*

### 3.5.4 Modbus/TCP en la práctica

De la teoría a la aplicación practica: el siguiente ejemplo explica la estructura de una petición y una respuesta para el código de función 03 “Lectura de los registros internos (Reading of internal Registers)”. La *Tabla 3-7* ilustra la estructura general de la petición, respuesta y mensaje de error. Los códigos de excepción dentro del mensaje de error se caracterizan por lo siguiente:

01 – código de función no valido
02 – Dirección no valida
03 – Valor no valido
04 – Error del dispositivo del servidor

| Petición | | |
|---|---|---|
| Código de función | 1 Byte | 0x03 |
| Dirección de Inicio | 2 Bytes | 0x0000 bis 0xFFFF |
| Numero de Registros | 2 Bytes | 1 up to 125 (0x7C) |

| Respuesta | | |
|---|---|---|
| Código de función | 1 Byte | 0x03 |
| Dirección de Inicio | 1 Byte | 2*N (Numero de registros transmitidos) |
| Numero de Registros | 2 Bytes | |

| Mensaje de Error | | |
|---|---|---|
| Código de Error | 1 Byte | 0x83 |
| Código de Excepción | 1 Byte | 01, 02, 03 or 04 |

***Tabla 3-7 Código de función 03 “Lectura de Registros” en detalle***

Como ejemplo del uso de los códigos de función mencionados anteriormente ahora los registros 108 (conteniendo el 555 en decimal y respectivamente 0x022B en hexa), 109 (conteniendo 0 y 0x000) y 110 (conteniendo 100 y 0x0064) serán leídos.
La estructura de la petición y respuesta esta dada en la *Tabla 3-8*. En este contexto debería ser recordado que el ejemplo manejado primero serviría para explicar la estructura general de las transacciones Modbus/TCP. Para el usuario el uso es siempre transparente – dependiendo del camino de la implementación del protocolo. Esto significa disparar lanzar una petición a un servidor este siempre tiene que parametrizar los bloques de función respectivos los cuales están predefinidos por el fabricante del dispositivo.

| Petición | | Petición | |
|---|---|---|---|
| Nombre de campo | (Hex) | Nombre de campo | (Hex) |
| Código de función | 03 | Código de función | 03 |
| Dirección de inicio (orden mas alto) | 03 | Numero de bytes | 03 |
| Dirección de inicio (orden mas bajo) | 03 | Contenido del Registro 108 (orden mas alto) | 03 |
| Numero de registros (orden mas alto) | 03 | Contenido del Registro 108 (orden mas bajo) | 03 |
| Numero de registros (orden mas bajo) | 03 | Contenido del Registro 109 (orden mas alto) | 03 |
| | | Contenido del Registro 109 (orden mas bajo) | 03 |
| | | Contenido del Registro 110 (orden mas alto) | 03 |
| | | Contenido del Registro 110 (orden mas bajo) | 03 |

***Tabla 3-8 Ejemplo sencillo para la petición de “Lectura de Registros”***

La descripción detallada del protocolo Modbus (así como para TCP/IP y para transmisión serial) incluyendo todos los códigos de función públicos pueden ser tomados desde la especificación mencionada del protocolo Modbus. Además en la página web del fabricante se ofrecen códigos de ejemplo para la implementación de protocolos en ciertos dispositivos. Las cosas que se dicen de Modbus/TCP – al ser similar a otros protocolos basados en TCP – no están limitadas solamente a Ethernet. Este es capaz de usarse en Internet o intranets, considerando a Ethernet para conexiones en redes telefónicas y transmisiones sin cables son también utilizables.

También la configuración de Firewalls es posible sin ningún problema por el IANA (Internet Assigned Numbers Authority) asignando uno de los llamados y bien conocidos “Puertos” (Puerto 502) para Modbus/TCP. Modbus/TCP esta óptimamente preparado no solo para aplicación en redes locales de automatización.

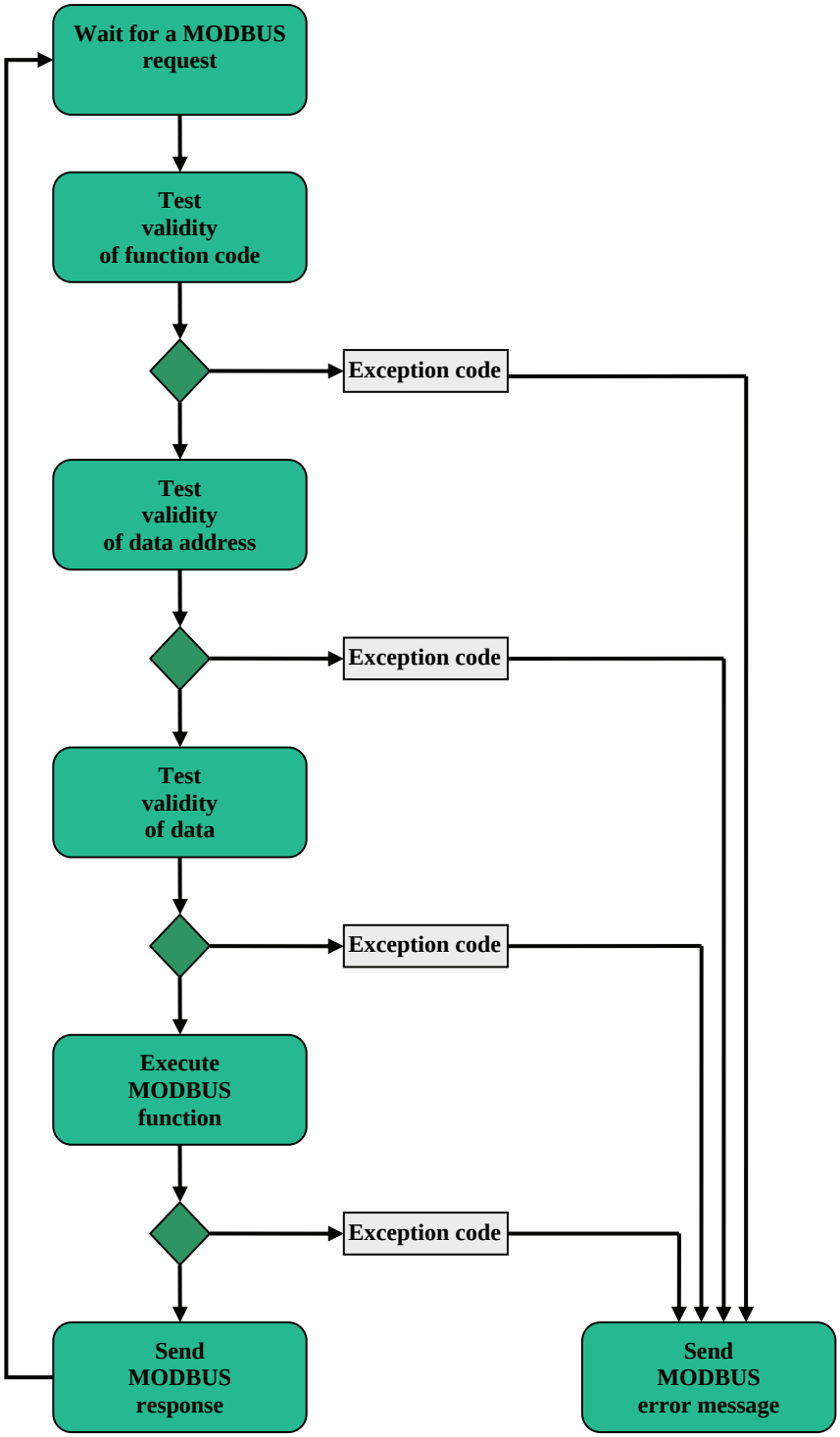



*Figura 3-32 Diagrama de estado de una transacción Modbus*

## 3.6 SERCOS III

SERCOS, la interfaz de drive digital, ha llegado a ser mundialmente aceptada como estándar de red para control de movimiento en la última década. SERCOS es particularmente interesante debido a sus características técnicas sobresalientes como habilidades de tiempo real, rendimiento, inmunidad al ruido y además la variedad de productos y distribuidores. La formula de la tercera generación de SERCOS es la combinación física y del protocolo Ethernet con los probados mecanismos de la interfaz SERCOS. Esta combinación ofrece nuevas y potentes opciones para la futura tecnología de control de movimiento.

### Introducción a SERCOS

La interfaz SERCOS fue desarrollada a mediados de los 80's por un consorcio industrial soportado por la "Verein Deutscher Werkzeugmaschinenfabriken e. V." (VDM) y la "Zentralverband Elektrotechnik und Elektroindustrie e. V." (ZVEI). La primera generación de la interfaz SERCOS soportaba tasas de transmisión de 2 a 4 Mbit/s y fue principalmente usada en aplicaciones de herramientas avanzadas. En los años siguientes SERCOS llego a ser mas y mas aceptado a nivel mundial y ha sido utilizada en todo tipo de aplicaciones servo-drive distintas. En 1995 la interfaz SERCOS fue establecida como la norma IEC 61491. En 1999 la segunda generación fue lanzada. La tasa de transmisión fue incrementada desde los 8 a los 16 Mbit/s y el canal de servicio para la transmisión de datos asíncronos fue extendido. Esta nueva tecnología ha estado disponible desde el 2001 basado en el SERCON816 ASIC, mientras que la compatibilidad descendente con la primera generación fue mantenida. Esto ofrece un rendimiento excepcional debido a las transmisiones libres de colisión basadas en mecanismos de slot de tiempo y un protocolo altamente eficiente, combinado con un comportamiento de tiempo absolutamente deterministico. Por ejemplo: hasta 40 ejes pueden ser sincronizados exactamente con un ciclo de tiempo de 1ms y una fluctuación de <1µs. Las fibras ópticas proveen una inmunidad máxima al ruido.

Gracias a sus habilidades técnicas y su amplio uso, SERCOS ha llegado a ser el estándar de facto en muchas ramas, especialmente para servo aplicaciones altamente dinámicas con muchos ejes, por ejemplo imprimiendo o empacando maquinas. Aunque la interfaz SERCOS fue originalmente diseñada como una mera interfaz de drive, esta es considerada hoy en día una interfaz de control de movimiento universalmente aplicable. La interfaz SERCOS no solo define un sistema de comunicación en tiempo-real sino también especifica más de 500 parámetros estandarizados los cuales dan una semántica de vendedor neutral para la interoperabilidad de controles y drives. Además de drives, estaciones de E/S están siendo conectadas al bus, así que la mayoría de las maquinas autónomas no requieren un fieldbus adicional.

Alrededor del mundo más de 50 fabricantes de controles y 30 fabricantes de drives ofrecen dispositivos compatibles con SERCOS. El Grupo de Interés de la Interfaz SERCOS (IGS, Interest Group SERCOS interface) con sus oficinas principales en Sttutgart, Alemania, tiene mas de 60 compañías miembros en el mundo y están representadas en Norteamérica y Japón con diversas organizaciones.

La tercera generación de la interfaz SERCOS (SERCOS III) es una evolución de los estándares SERCOS existentes (IEC/EN 61491), basados en el estándar Ethernet. Los conocidos y probados mecanismos SERCOS como por ejemplo: los perfiles de control de movimiento, la estructura del telegrama y la sincronización de hardware han sido mapeados al estándar Ethernet. Para asegurar los altos requerimientos de tiempo-real a pesar del uso de Ethernet, SERCOS III usa un canal adicional de tiempo-real libre de colisiones que es paralelo al canal IP estándar. En este canal de tiempo real libre de colisiones los telegramas SERCOS definidos son transmitidos. La alta eficiencia del protocolo en este canal asegura el mejor rendimiento aun con un alto número de participantes y datos pequeños por dispositivo. Un canal IP puede ser configurado paralelo a este canal de tiempo real en el cual telegramas Ethernet o de protocolos basados en IP como TCP/IP o UDP/IP pueden ser transmitidos.

### 3.6.1 Características distintas de SERCOS III

El revolucionario concepto de SERCOS III mantiene las bien conocidas y probadas ventajas y al mismo tiempo un rango de nuevas características las cuales permiten el sustancial incremento del número de aplicaciones:

- Protección de las inversiones debido a la alta compatibilidad con la interfaz previa SERCOS (topología, perfiles, estructuras de telegrama, sincronización)
- Reducción de los costos del hardware para una interfaz de conexión SERCOS III en el nivel de una interfaz análoga
- Integración a protocolos IP
- Comunicación cruzada entre esclavos
- Sintonización de diversos controles de movimiento
- Transferencia de datos relevantes de forma segura
- Tolerancia a las fallas en caso de interrupción óptica

A continuación se da una descripción mas detallada de algunos de los puntos siguientes:

### 3.6.2 Topología

SERCOS III soporta una estructura en anillo, como en la primera y segunda generación de esta interfaz. Características condicionales en la física de Ethernet para full-duplex, no obstante, no en una estructura sencilla, pero si en una de doble anillo. Esta estructura de doble anillo ofrece la posibilidad de transferir datos redundantemente.

En caso de una ruptura de la fibra en cualquier punto del anillo la comunicación sigue funcionando. La maquinaria sigue trabajando mientras la herramienta de diagnostico integrada señala la falla, la cual puede ser reemplazada sin interferir con la disponibilidad de la maquinaria.

Además la estructura en anillo una estructura lineal también es posible. La estructura lineal, sin embargo, no ofrece la ventaja de la redundancia, pero si ahorra en el cableado de las conexiones. SERCOS III no usa una topología en estrella del Ethernet estándar y por lo tanto hubs o switches no son necesarios. Tiempos de retardo y fluctuaciones son reducidos al mínimo en todos los nodos procesando datos en tiempo real “al vuelo” (on the fly).

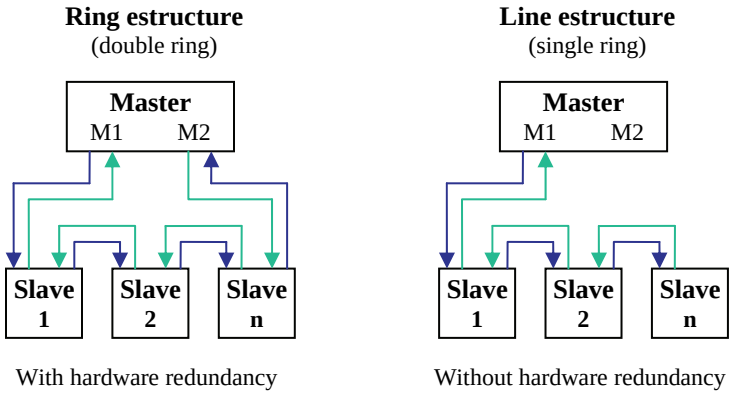


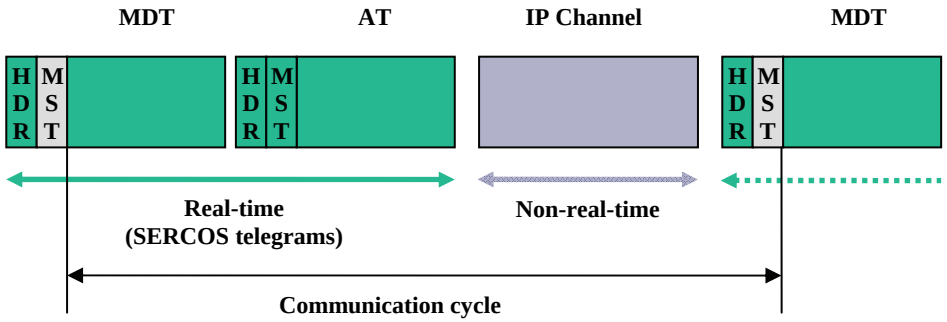

***Figura 3-33 Topología de SERCOS***

La instalación de una red SERCOS es muy sencilla y no requiere ningún procedimiento de configuración específico. Todos los nodos son simplemente conectados por patch-cables o cables crossover. Los puertos Ethernet de los dispositivos son intercambiables y pueden aun ser usados para conectar nodos Ethernet estándar (por ejemplo laptops) a un dominio de tiempo real SERCOS.

En este caso, se da conectividad completa tanto Ethernet como IP, pero el comportamiento de tiempo real no se afecta.

### 3.6.3 Canal deterministico de tiempo real y canal IP

El control maestro y los esclavos pueden intercambiar configuraciones de comunicación, parámetros o datos de diagnostico vía el llamado canal de servicio. Por razones de compatibilidad este canal continúa sin cambios en SERCOS III. Un canal IP adicional puede correrse para la transmisión de tramas Ethernet estándar como telegramas TCP/IP o UDP/IP. Los ciclos de tiempo, así como el particionamiento del canal cíclico y el canal IP pueden ser ajustados a los requerimientos específicos de la aplicación.




MDT, AT and IP channel telegrams are embedded in Standard Ethernet frames

***Figura 3-34 Estructura del protocolo con SERCOS III***

### 3.6.4 Comunicación de control de movimiento para el concepto de drives centrales y no centrales

SERCOS III divide a la mitad el tiempo mínimo de ciclo de actualmente 62.5 µs a 31.25 µs. Debido al gran ancho de banda en la física de Ethernet esto sigue siendo posible para conectar un número adecuado de esclavos, debido al bajo ciclo de tiempo. Esto permite la implementación de concepto de drives descentralizados igual de bien que con un procesamiento central de señal. Con un concepto de drive descentralizado todos los bucles de control se encierran en la unidad de control de drive.
Con conceptos centrales solo el bucle actual se encierra en el drive, mientras todos los demás bucles de varios ejes son implementados en un control central electrónico.

### 3.6.5 Sincronización de controles de movimiento y comunicación directa entre esclavos

Debido a la comunicación unidireccional en la fibra óptica, una comunicación directa entre los esclavos no esta soportada con la primera y segunda generación de la interfaz SERCOS. SERCOS III, no obstante, soporta esta característica de comunicación cruzada la cual es ventajosa para varias aplicaciones de control de movimiento.

La comunicación y sincronización entre múltiples controles de movimiento también esta llegando a ser mas y mas importante. La tendencia hacia la modularización requiere conceptos de control de movimiento que ofrecen la posibilidad de sincronizar varios módulos de maquinas y para intercambiar datos de tiempo real.
SERCOS III también soporta el incremento de funciones de seguridad importantes. Con SERCOS III, los datos seguros y no seguros se transfieren con los mismos mecanismos.

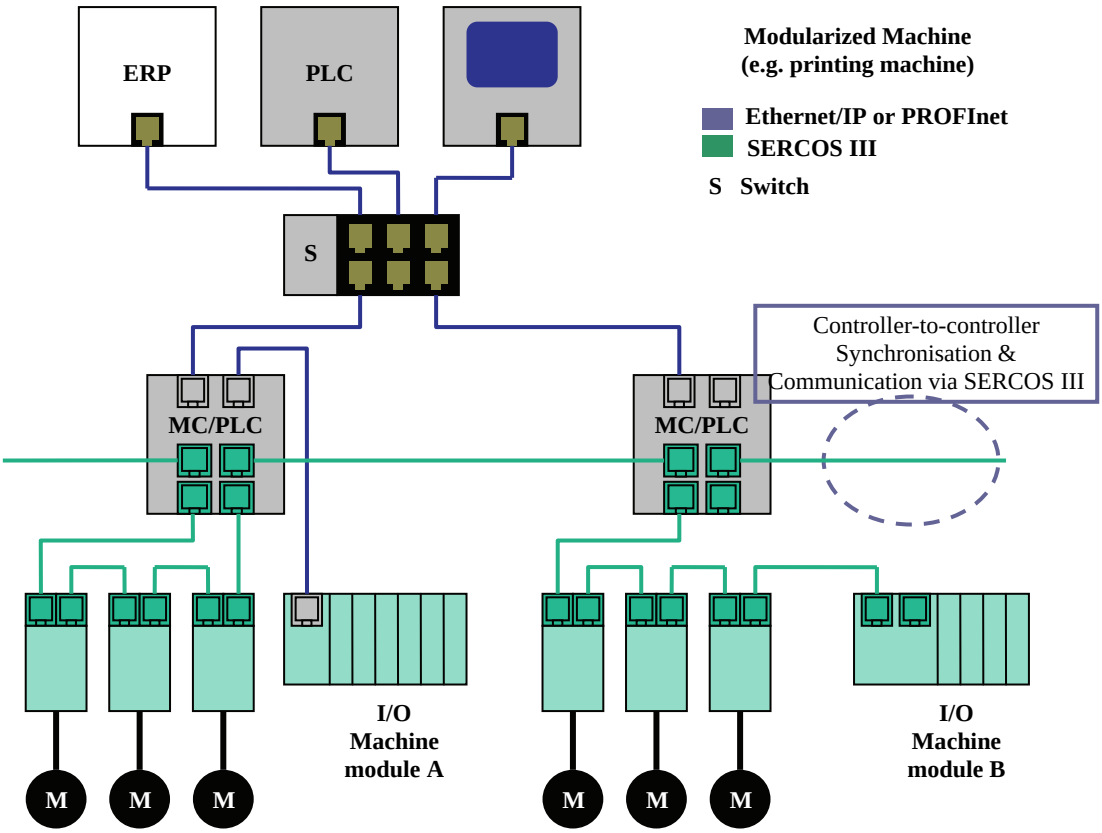



*Figura 3-35 Sincronización de varios controls de movimiento via SERCOS III*

### 3.6.6 Hardware SERCOS III

La primera y segunda generaciones de SERCOS han estado soportadas por un ASIC especifico de comunicación (SERCON 410B y SERCON 816). Con SERCOS III una solución de hardware más flexible es usada. La base es el desarrollo del núcleo SERCOS (SERCOS III IP), con la cual el control de comunicación basada en FPGA SERCON100 es realizado. Sumado a esto, fabricantes de componentes y sistemas son capaces de integrar la funcionalidad del hardware SERCOS III a sus propios componentes lógicos en un FPGA común. Además, el grupo de interés de la interfaz SERCOS coopera con los fabricantes de chips y casas de sistemas con el fin de integrar las funciones requeridas de hardware y controladores de comunicación multiprotocolo universalmente (por ejemplo el controlados netX de Hilscher). Estos controladores soportan varios protocolos Ethernet industriales solo con ajustar el software controlador.
Esto es una ventaja no solo para los fabricantes de componentes; también los OEM necesitan manejar solo un tipo de cableado. El usuario final se beneficia al no tener que usar diferentes configuraciones de hardware, en caso de que el este usando diferentes protocolos Ethernet industriales en su planta. Una meta esencial del nuevo hardware SERCOS III es la reducción de costos por nodo. Dos hechos intervienen:

- ASIC no especial, pero módulos estándar como FPGA o controladores de comunicación
- Acoplamientos Ethernet en vez de acoplamientos de fibra óptica, lo que significa menores costos de plugs

Estos hacen a SERCOS III una interesante opción también en productos sensibles de mucho costo.
Continúa soportado el acoplamiento de dispositivos ópticos con el fin de tener una solución con la máxima inmunidad al ruido y cobertura de larga distancia.

| Datos cíclicos | Ciclo de tiempo | No. de dispositivos | Tipo de datos cíclicos |
|---|---|---|---|
| 8 Byte | 31.25 µs | 8 | Punto de referencia de Torque, posición actual |
| 12 Byte | 250 µs | 70 | Punto de referencia de velocidad y valor actual, posición de referencia y valor actual |
| 32 Byte | 1 ms | 150 | Numerosos puntos de referencia y valores actuales |
| 16 Byte | 1 ms | 254 | Numero máximo de dispositivos |

***Tabla 3-9 Rendimiento SERCOS III***

### 3.6.7 Migración de SERCOS II a SERCOS III

La interfaz SERCOS tiene una buena tradición lanzando nuevos pasos para evolucionar. La migración desde la primera a la segunda generación, por ejemplo, solo requería un cambio en el hardware.
Esta tradición continúa con SERCOS III, de este modo se protegen las inversiones de los usuarios SERCOS.

**- Migración paso 1.** Reemplazar las fibras ópticas físicas con las físicas Ethernet.
Un cambio en el hardware es necesario pero los fabricantes de componentes SERCOS solo tiene que hacer pequeños cambios en el software, si solo el canal cíclico tiene que ser utilizado. La transmisión exclusiva de los mecanismos tradicionales SERCOS es el paso de implementación mínima y es por lo tanto la parte obligatoria de SERCOS III.

**- Migración paso 2.** Utilizando las posibilidades mejoradas de SERCOS III. Sumadas al paso 1 las nuevas funciones definidas en SERCOS III pueden ser usadas: Canal IP, comunicación cruzada, transferencia de datos segura, etc.

### 3.6.8 Entrada directa a SERCOS III

Para aquellos que usen SERCOS por primera vez y comiencen directamente con SERCOS III, starter kits y drivers de software para maestros y esclavos están disponibles. Esto hace el primer uso de la interfaz SERCOS tan fácil como es posible.

### 3.6.9 Clases de tiempo real cubiertas por SERCOS III

La *Tabla 3-10* muestra diferentes tipos de comunicación para la industria de la automatización. Éstas están clasificadas en cinco tipos de tiempo real. La figura muestra la cobertura provista por las diferentes generaciones de la interfaz SERCOS. SERCOS III cobre todas las áreas relevantes de tiempo real. La comunicación Ethernet estándar también ésta también incluida, si el cana IP es usado sin el canal cíclico de tiempo real.

| | Tiempos de Ciclo | Requerimientos de Sincronización | SERCOS I, II | SERCOS III |
|---|---|---|---|---|
| Comunicación Ethernet estándar | No cíclico | No Sincronizado | | |
| Drives de posición, FCs, I/Os… | 4 … 10 ms | > 4 ms | | |
| Comm. & Synchro. Controller-to-controller | 1 … 10 ms | 1 … 10 ms | | |
| Drives coordinados, High speed I/Os. | 250 µs … 4 ms | < 1 µs | SERCOS I SERCOS II | SERCOS III |
| Conceptos de drives Multi-ejes con procesamiento de señal centralizada | 31.25 µs … 125 µs | < 1 µs | | |

***Tabla 3-10 Comparación de cobertura entre SERCOS I, II y III***

## 3.7 Caso de aplicación 1 – Red unificada para VW

Volkswagen Saxony GmbH en Mosel Alemania fabrica cerca de 1,000 automóviles al día. El ensamble del Passat y del Golf con las especificaciones que el consumidor requiere así como las áreas de producción y administración están totalmente integradas vía redes sobre las cuales corren aplicaciones como son archivos y servicios de impresión, bases de datos especificas como Oracle, DB2, Microsoft SQL, sistemas SAP R/2 y R/3, emulaciones SNA-3270 para la computadora central, aplicaciones basadas en web, sistemas de e-mail, intranet e Internet, acceso en línea a recursos del grupo corporativo en los centros de computo de Wolfsburg e Ingolstadt.

La red de comunicaciones tiene más de 50 servidores corriendo Windows NT o Unix y esta basada extensivamente en los productos Hirschmann. Esta red tiene 1,200 usuarios en un área de 1.8 $Km^2$. Todos los edificios están incluidos y el largo total es de 1,000 Km, de los cuales cerca del 70% es fibra óptica.

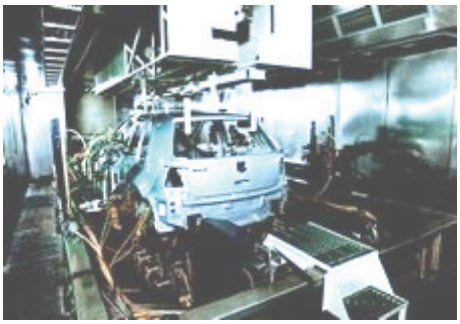


***Figura 3-36: Línea de ensamble del Golf en Mosel, Alemania***

Fibra óptica mono-modo ha sido recientemente instalada para Gigabit Ethernet. Fibra óptica multi-modo es también utilizada en el cableado estructurado (backbone, edificios y pisos).

El director de Organización y Coordinación IS de la fabrica, Mathias Mueller, acentúa: “La red debe estar 100% disponible las 24 horas al día, los 365 días al año. Esto es muy importante y en general nosotros no hacemos distinciones entre la red de la fábrica y la de la oficina. Y no debe haber diferencias de calidad tampoco.

“Estamos intentando desarrollar la red de manera que estemos listos para instalar las futuras aplicaciones”.

“La redundancia es importante porque no podemos hacer un ‘chequeo ligero’ debido a las distancias. Tenemos que ser capaces de restaurar la funcionalidad de la red automáticamente en caso de una falla. Las estructuras redundantes hacen esto posible para nosotros y así se apoya a la red con personal en sitio entre las 6 a.m. y 6 p.m. Este concepto, junto con el monitoreo central de la red y el software de administración de la red, se adecua bien con nuestra estrategia y ha sido probada por si misma en la practica”.

Los requerimientos de redundancia alcanzan gran significado con el ancho de banda dado por Gigabit Ethernet para el GRS. La protección contra fallas proporcionada por el equipamiento Hirschmann y el relativo fácil manejo y control de la tecnología Ethernet también jugo un rol importante en la decisión de tener a Gigabit Ethernet en el backbone. La implementación de Gigabit Ethernet tomo 16 semanas desde la planeación hasta la implementación. En el futuro, está hará posible vincular aplicaciones de video y usuarios adicionales en la red de datos.

## 3.8 Caso de aplicación 2 – BMW toma el bus sobre Ethernet

Un dólar débil no solo es la razón por la que la producción basada en Estados Unidos esta jugando un rol importante en la industria automotriz. La creciente importancia de Estados Unidos ha reaccionado de regreso a los planeadores de las tecnologías de sistemas de control del Centro de Innovación e Investigación del Grupo BMW (BMW Group's Research and Innovation Centre, Forschungs - und Innovations Zentrum) FIZ en Munich, Alemania. FIZ ahora encara el reto de convenir estándares comunes con sus colegas americanos. Y estos estándares tienen que reconciliar el deseo de usar una tecnología de sistemas de control por un lado y por el otro asegurar la eficiencia económica de los estándares instalados.

***Figura 3-37: Instalaciones de producción BMW Spartanburg, Carolina del Sur***

La prensa automotriz especializada esta llena de reportes exponiendo que el futuro de la producción automotriz para el mercado norteamericano estará basada en los Estados Unidos. También la persistencia de la debilidad del dólar no solo es la razón para esto. Cuando se está en el mercado norteamericano es más una cuestión de imagen. Para muchos ciudadanos americanos una decisión para adquirir un producto depende del lugar de origen del mismo. En otras palabras si esta "Hecho en USA".

Otra ventaja de fabricar en el país que se consumirá el producto es que, si las capacidades de producción son distribuidas de forma correcta y se cumple con la demanda local, los costos de transportación para vehículos ya ensamblados pueden reducirse. Consideraciones similares influenciaron la principal decisión de la BMW para fabricar unas series de vehículos deportivo-utilitarios (SUV, Sport Utility Vehicle) en Spartanburg, Carolina del Sur. Estas incluyen los Z3, X5 y desde 2002 los Z4.

Alrededor de 130,000 vehículos han salido de la línea de producción anualmente en la planta Spartanburg desde que inicio operaciones en 1994. Sin embargo, cualquier instalación es tan buena como la gente que la opera y mantiene. Así proveyendo entrenamiento y transfiriendo conocimiento acerca de la tecnología del sistema de control preferido en Alemania involucra un costo considerable. Para limitar este gasto, BMW Spartanburg ha implementado una tecnología de Controlador Lógico Programable (PLC) Rockwell. Esto no significaba que automáticamente BMW tenía precedentes de las ventajas de la comunicación fieldbus y la correspondiente tecnología de instalación. La filosofía de diseño abierto detrás del sistema Phoenix Contact's Interbus dio la integración con los productos controladores Rockwell.

### 3.8.1 Ethernet satisface a Interbus

Un puente de comunicación inteligente fue asignado en el modulo de interfaz para el Control Logix SST IBS CLX RLL. Esta solución retenía las ventajas ofrecidas por acceso directo desde el software de aplicación diseñado para la planta, por ejemplo para una aplicación de soldadura, mientras se evitaban nodos Ethernet adicionales y más caros. Parámetros, diagnósticos y aun archivos de datos para el sistema de control de soldadura o datos para un convertidor de frecuencia pueden así ser intercambiados directamente vía Interbus y la Ethernet sin la necesidad de módulos de función extras.

Los datos de configuración y diagnostico para las tarjetas controladoras y acopladores de sistema usados en los robots pueden ser accedidos también directamente. El modulo de interfaz usa el bus Control Logix y la conexión Ethernet ya provista en el rack para la transmisión de datos al nivel HMI (Human Machine Interface).

La conexión Ethernet es también usada para programar y visualizar los datos de los PLC. Un reloj con una velocidad de 2 MBaudios asegura los suficientes niveles de rendimiento para este incremento del volumen de datos en el fieldbus.

### 3.8.2 Espacio compacto por diseño

Como fue el caso para la producción de las Series 7 BMW, BMW quería asegurar que el espacio limite en Spartanburg fuera actualmente usado para la producción – y no solo almacenando dispositivos de switcheo. Esto significo que la compañía solo quería un gabinete de control en las proximidades directas de cada parte de la planta. Este gabinete tenia que incluir la alimentación eléctrica, controladores, sistema de control de seguridad y el sistema de visualización y dispositivos operantes. Todos los demás dispositivos como convertidores de frecuencia, arrancadores de motor y E/S's fueron implementados localmente.

***Figura 3-38: Gabinete de control en las instalaciones de Spartanburg***

La solución para esto estuvo basada en la tecnología Phoenix Contact's Rugged Line. La categoría de protección inherente IP67 asegura que las tuberías de enfriado y similares no representaran riesgo por daños en el sistema, aun durante mantenimiento. Una multitud de LED's de diagnostico han sido integrados en la caja robusta fundida con Zinc. Al lado de la señalización de una falla de alimentación, también se provee información en un canal específico acerca de fallas en los sensores. Una placa montada y enchufes fáciles de usar también hacen más fácil el intercambio de partes. Estos salvan costos de inactividad e incrementan la disponibilidad de la planta de producción.

Los arrancadores de motor aprobados IBS IP480 MLR usados para el sistema de control de vía de suspensión electrónica también pertenece al rango Rugged Line. Las E/S del sistema Inline son solo usadas en las pequeñas cajas de switch así como en el gabinete del sistema de visualización. Usando tecnología por partes, las estaciones de E/S pueden ser puestas juntas como es requerido.

### 3.8.3 Diseño en base a fibra óptica

A inicios de 1999, BMW decidió implementar tecnología de cable de fibra óptica a través de sus líneas de producción de autos. La razón decisiva para hacer esto en primera instancia fue evitar fallas causadas por interferencias EMC. Teniendo probado su valor funcional bajo condiciones de prueba y reales, esta tecnología tenía la ventaja de que las fibras de polímero daban un fácil ensamble en comparación con el cobre.

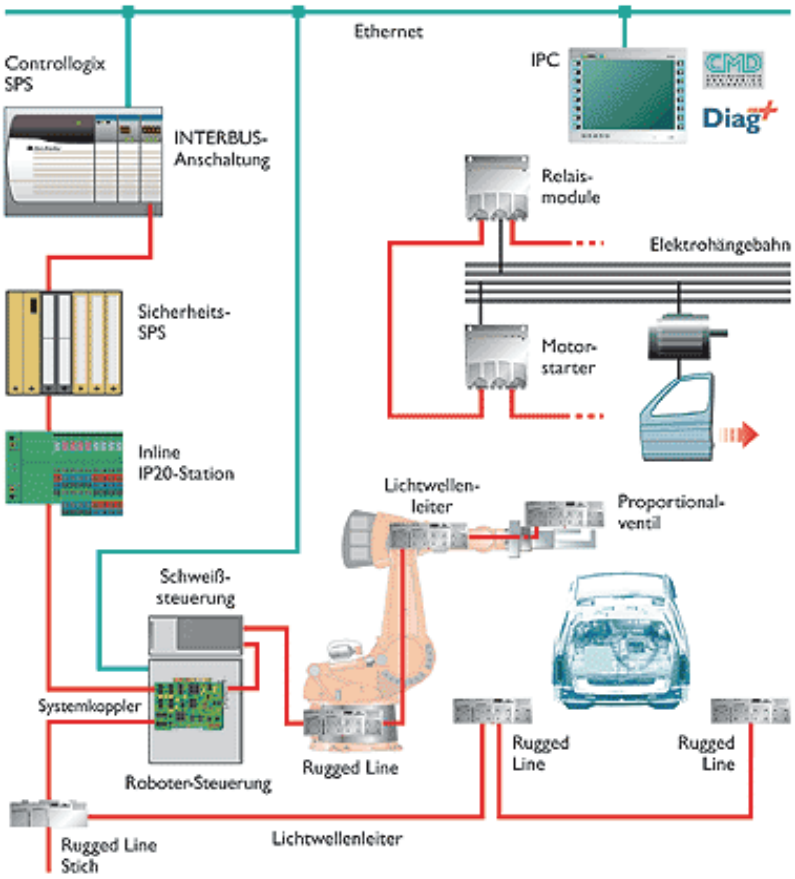



***Figura 3-39: Topología del sistema de control y concepto de comunicación***

El desarrollo de cables de arrastre y resistentes a la corrosión significo que estos también podían ser instalados en las partes móviles de los robots.

Utilizando un control de intensidad luminosa de 15 niveles para los diodos láser en los dispositivos Interbus también extiende la vida de servicio del recipiente y sirve para proveer alerta temprana en el evento de degradación de la línea física. Si la calidad decrece, por ejemplo en el área del sistema de reserva, un software de diagnostico o las banderas de la herramienta de configuración CMD prenden la línea de mantenimiento personal. Estas cabeceras de apagado no programado y la línea pueden ser intercambiadas durante una oportunidad en el mantenimiento programado.

Dispositivos adicionales también fueron desarrollados para cumplir un rango de tareas especiales. Desde las islas de válvulas a las válvulas proporcionales, desde los cambiadores de herramientas a los conectores rotatorios – el diseño de esta instalación representa un portafolio de producto completo proporcionado por varios proveedores.

### 3.8.4 Software de soporte

Como en Munich, la instalación de Spartanburg también da un gran valor al soporte del software. En dialogo con la industria automotriz, Phoenix ha desarrollado el @utomation Xplorer, CMD y herramientas de software Diag+ para establecer y mantener plantas. Aquí, CMD es generalmente usado para configurar y establecer los sistemas Interbus. Y esto les significa a los usuarios estar ya en posición de realizar tareas desde líneas de cable de fibra óptica para imprimir un certificado para la entrega de la planta.

El software @utomation Xplorer, el cual utiliza datos CMD, muestra una visión en cascada de los sistemas de bus en una estructura de árbol. Todos los dispositivos inteligentes de red como son convertidores de frecuencia o los sistemas controladores de soldadura pueden ser accedidos directamente seleccionando el software de aplicación del producto específico. En una emergencia, este dispositivo permite al usuario orientarse el mismo y localizar errores. Al mismo tiempo, la herramienta maneja direcciones de comunicación entre Ethernet e Interbus así como desde los subsistemas Interbus al nivel de robots.

***Figura 3-40: Brazo de robot en la línea de ensamble***

La herramienta Diag+ ofrece soporte directo para personal de mantenimiento de la planta. Este coteja todos los datos de diagnostico relevantes e inhibe el hacer cualquier cambio por error. Como un producto competente ActiveX, este podría también ser integrado en los sistemas de visualización existentes con un mínimo esfuerzo – y sin necesidad de que los usuarios inserten sus propios mensajes de error o gasten grandes montos de tiempo conectando mensajes de error en las tablas de datos de los PLC's. Paul Cresswell, especialista en controles y soldadura en la planta BMW de Spartanburg menciona que el sistema Interbus ayuda a prevenir apagados en la planta "sin tener que sacrificar nuestro conocimiento y experiencia usando una tecnología de sistemas de control familiar".

Robert Haller de FIZ y Warren Widener, especialista senior en controles y soldadura de la BMW de Spartanburg dice que el punto de vista de Cresswell describe una de las precondiciones para implementar Interbus como una solución global estándar en las líneas de producción BMW. "Sumado a esto, Phoenix Contact fue un gran socio para trabajar con sus servicios y soluciones ofreciendo el balance correcto entre el uso de soluciones en sistemas de control preferidos localmente, instalaciones de mantenimiento y estándares de comunicación en el campo".

## 3.9 Caso de aplicación 3 - Para trabajar 5 años sin interrupciones en BASF

Cubriendo un área de más de 7 $Km^2$, las instalaciones de BASF en Ludwigshafen es el lugar que maneja químicos más grande del mundo. De acuerdo con su concepto *Verbund* – es el distintivo de BASF para acercarse a la integración – la compañía produce 8,000 productos diferentes solo en este sitio. *Verbund* literalmente significa 'conectado'. La producción involucra tomar un número mínimo de materiales del almacén y usar estos para fabricar varias docenas de materiales básicos, los cuales son usados para producir cientos de productos intermedios. Estos productos intermedios entonces pasan a través de una red de producción de valor agregado y después por cadenas de proceso para producir varios productos terminados.

### 3.9.1 Alta disponibilidad

La energía de la red y los datos del flujo de material se hacen por el uso eficiente de los bienes pero requiere logística y administración de la producción inteligentes.
La producción de plásticos, una de las principales actividades en Ludwigshafen, trabaja 24 horas al día sin interrupción año con año. Interrupciones del proceso y reinicios de producción son muy costosos en términos de tiempo y pérdida de energía. Si un reinicio es requerido, este tomara varias horas antes de que el plástico con el perfil deseado y parámetros de calidad pueda ser producido una vez mas. Como el proceso del plástico es intencionalmente parado para propósitos de inspección solo una vez cada 5 años, las demandas requeridas para el sistema de control y la red de comunicaciones son increíblemente altas.

Cuando se modernizo la instalación del sistema de control de procesos, BASF planeo escoger una estructura Ethernet redundante basada en switches de Línea de Fabrica (Factory Line Switches) de la firma Phoenix Contact. La operación se extiende sobre dos edificios así como en el tanque de productos y al área del silo. Esto comprende varios cuartos de switch en el área de proceso, dos cuartos de control y una estación de configuración. Para cumplir los altos requerimientos de disponibilidad, los switches de Línea de Fabrica fueron conectados a un anillo Ethernet redundante en todas las locaciones. Si una conexión de red falla, el mecanismo redundante automáticamente activa la trayectoria alterna en el anillo. En adición a esto, la estructura en anillo habilita la expansión para ser llevada a cabo desde cualquier locación del sistema sin incurrir en tiempos muertos, esencial para la operación continua.

Como con otros componentes cerrados a los dispositivos de proceso de E/S, los switches Ethernet son montados directamente en el rail DIN dentro de los cuartos de switch. El equipo tiene que compartir la ocupación del cuarto con un inversor de alta frecuencia entregando más de un MegaWatt de potencia. Con compatibilidad completa absolutamente esencial los backbones Ethernet utilizan tecnología de fibra óptica.

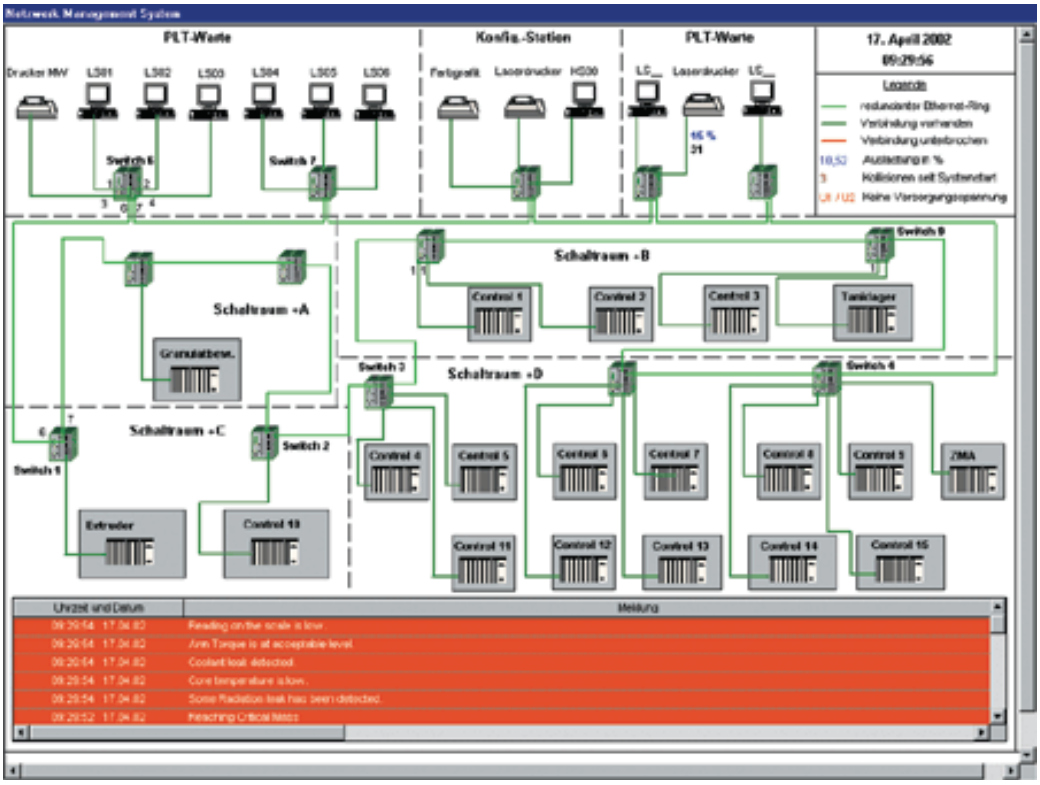



*Figura 3-41: Visualización del software Génesis para monitoreo y diagnósticos. Esta vista muestra la red completa con dispositivos individuales y la estructura de la topología*

### 3.9.2 Planeación y diseño

La planeación e implementación de Ethernet industrial a esta escala fue una nueva experiencia para BASF. Phoenix Contact ayudo proveyendo tanto los componentes Ethernet industriales así como el servicio de diseño para el productor químico.
Los paquetes de tareas específicos fueron usados durante la instalación, inicio y configuración de la red basada en el software Phoenix Factory Manager. Habiendo sido dada una breve inducción, el entrenamiento básico posibilita a los ingenieros de planta de BASF a hacer sus propios cambios a la configuración y llevar a cabo la expansión del sistema.

### 3.9.3 Visualización de red

BASF usa dos mecanismos para mantener un rastro de la operación del sistema usando información provista por los switches. Cuando un componente de la infraestructura falla, los switches son configurados como vía que en un contacto eléctrico aislado genera un mensaje de grupo si un dispositivo conectado es removido desde un puerto, la redundancia sobre el switch es activada o algunos otros errores ocurren. Los mensajes de error son enviados inmediatamente al cuarto de control.

Información adicional y mensajes relacionados a los switches vienen vía SNMP (Simple Network Management Protocol). La función SNMP da información acerca de switches individuales y la red en términos del puerto leído, conexión y status de redundancia. Estos datos son automáticamente archivados. Los switches también reportan trampas SNMP independientemente en eventos relevantes. Esta información de eventos llega a estar disponible a través de la red entera.

El software de visualización Génesis, el cual es provisto con administración de información relevante vía el servidor SNMP OPC, es usado para monitoreo de la red y diagnósticos en el cuarto de control. El diagrama de visualización muestra la red entera con dispositivos individuales y la estructura de la topología. Información como el estado de conexión, capacidad y colisiones es provista a los puertos individuales y pueden ser accedidos colectivamente.
Esto hace posible el detectar cuellos de botella en una etapa temprana antes de que fallas de red costosas puedan ocurrir. Esto también provee a BASF de una buena administración con una base de datos para determinar si requerimientos y propiedades de la operación de producción pueden ser atendidos por la red.

A un año de iniciar la operación de la red basada en Ethernet, los administradores del sistema del gigante químico alemán han quedado impresionados.

| | EtherCAT | Ethernet/IP | Ethernet Powerlink | Modbus/TCP | SERCOS III |
|---|---|---|---|---|---|
| Vendor Organisation | ETG EtherCAT Technology Group | ODVA Open DeviceNet Vendor Association | EPSG Ethernet Powerlink Specification Group | Modbus-IDA Group | Interest Group Sercos Interface (IGS) |
| Homepage | www.ethercat.org | www.odva.org | www.ethernet-powerlink.org | www.modbus-ida.org | www.sercos.de |
| Availability of specification | ETG members | Freely available | EPSG members | Freely available | Specified within IEC 61491 and EN 61491 |
| Availability of technology | Examples code, ASIC or FPGA | Example code | Standard Ethernet chips, no special ASICS required | Example code | Planned: Sercos-core (SERCOS III-IP) for FPGA integration |
| Products available since | 2003 | 2000 | 2001 | 1999 | 2005 |
| Interaction structure | Master/Slave | Client/Server | Master/Slave | Client/Server | Master/Slave |
| Communication method | One frame for all communication partners, data stream processed during its path through | Message oriented and Common Package Format | Message oriented | Message oriented | Charred telegram |
| Real-time method | Isochronous | Clock synchronisation with CIPSync | Time slot, realised by polling | Implementation dependent | Time slot |
| Transmission of real-time data | Ethernet frames, alternatively UDP/IP possible | Public/Subscribe (Implicit Messages using standard IP frames) | Ethernet frames using broadcast messages | Standard IP frames | Ethernet frames |
| Transmission of non-real-time data | Protocol tunnelling | Explicit messages | Acyclic time slot | (No cyclic communication) | Acyclic time slot |
| TCP/IP Stack | Transparent on real-time Stack possible | Complete, no separate real-time stack | Parallel to real-time stack for acyclic data | Complete, no separate real-time stack | Parallel to real-time stack |
| Ethernet data transfer rate | 100 MBits/s | 100 MBits/s, 10 MBits/s | 100 MBits/s | 100 MBits/s, 10 MBits/s | 100 MBits/s |
| Physical topology | Line, Daisy Chain, Tree | Star | Star | Star, Tree | Double ring, Line |
| Logical topology | Open ring bus | Bus | Ring | Bus | Ring |
| Infrastructure components | Switches between different segments, within a segment connection over 2 ports (integrated in devices) | Switches (Hubs are possible but not efficient) | Hubs, no switches | Hubs, switches | Within a segment connection over 2 ports (integrated in devices) |
| Hardware solutions | Yes | No | Possible | No | Yes |
| Placement within the OSI model | Layer 2 | Above Layer 4 | Above Layer 2 | Above Layer 4 | Above Layer 2 |
| IP-address Resolution | Only for devices with IP address (usually one MAC address for one segment (first segment device)) | Up to devices | Up to devices | Up to devices | Up to devices |
| Device profiles | CANopen or SERCOS | DeviceNet (CAN), ControlNet | CANopen | No | SERCOS |

***Tabla 3-11 Compilación de los principales protocolos Ethernet***

# CONCLUSIONES

El uso de las redes de computadoras se ha ido extendiendo cada vez mas y mas debido a los múltiples usos que se les ha dado tanto en el uso militar, en la industria aeroespacial, en escuelas y facultades, en oficinas, en las casas y mas recientemente en la industria en la cual ha generado gran aceptación debido a las facilidades de implementación y puesta en marcha de los proyectos relativos. Es gracias a esta gran aceptación que para el uso de las redes de computadoras en la industria fue necesario el tratar de unificar el modo en como se comunicaban los diversos dispositivos dentro de las instalaciones para que así no fuera una necesidad el tener que realizar implementaciones extras para que uno o varios dispositivos específicos pudieran comunicarse con la red.

Ethernet fue el protocolo que ha sobrevivido a la larga lucha por estandarizar las comunicaciones no solo a nivel oficina, sino también a nivel industrial proporcionando un gran soporte de software y hardware generado por el desarrollo que se le dio en un inicio en la oficina, dando como resultado que casi con cada nueva implementación de tecnología de Ethernet a nivel oficina en el ámbito industrial se refleje esa misma para la versión Ethernet correspondiente.

Pero Ethernet industrial va más allá de las especificaciones requeridas para la oficina: proporciona no solo las tecnologías de conexión física (como la topología de bus, estrella o anillo), sino también estructuras de comunicación lógica (como la editor-suscriptor, la maestro-esclavo, la cliente-servidor, la cliente-servidor, etc.) así como comunicación en tiempo real debido a los tiempos de respuesta necesarios en operaciones criticas que se pueden dar en industrias como la química, la de semiconductores, la del cemento, etc.

Ethernet industrial al igual que su predecesor en la oficina implementa características de seguridad puesto que hoy en día todas las redes de computadoras a nivel mundial están bajo amenaza constante debido a la introducción de virus, hackeo, crakeo y demás tecnologías que obviamente ponen en peligro la integridad no solo de la red a nivel industrial, también de la red corporativa a la que pertenece el sistema pudiendo dar como resultado desde tiempos muertos de producción hasta el riesgo de accidentes producidos por la desconfiguración de los sistemas computarizados.

El protocolo Ethernet a nivel industrial ha sido tomado por distintas empresas que le han hecho modificaciones propias dando como resultado una gran variedad de subtecnologías mediante las cuales el consumidor del producto Ethernet tiene una amplia posibilidad de opciones a escoger tomando en cuenta la flexibilidad de la solución, los tiempos de respuesta para sus procesos críticos, la escalabilidad de productos, así como la amplia variedad de fabricantes de dispositivos de los cuales se puede comparar y comprar la mejor opción tanto para el presupuesto como para la robustez final del sistema implementado.

Algunos de los protocolos industriales aprobados que están basados en Ethernet según la IAONA (Industrial Automation Open Networking Alliance) que es la organización a nivel europeo encargada de organizar, extender y promover los estándares relativos al uso de Ethernet industrial son los siguientes: EPA (Ethernet for Plant Automation), EtherCAT (Ethernet for Control Automation Technology), Ethernet/IP, EPL (ETHERNET Powerlink), JetSync, Modbus-RTPS (Modbus Real-Time Publish Subscribe), P-NET on IP, PROFINET, SERCOS III, TCnet (Time-critical Control Network).

Ethernet a nivel industrial es el protocolo que hoy en día esta predominando en el mercado y por lo tanto es la tecnología a seguir por parte de todas las empresas, instituciones y gente relacionada con las comunicaciones a cualquier nivel, por lo tanto es nuestra obligación el tratar de conocer mas acerca de estos desarrollos ya que en un mundo cada vez mas globalizado el uso de las tecnologías debería ser una prioridad pues en la medida que un país y su gente este mas actualizados con los constantes cambios de infraestructura y procesos mas será la competitividad y grado de desarrollo dando como consecuencia un mejor país y una mejor forma de vida para sus habitantes.

# APENDICE

## *Números*

**10Base2**
Especificación Ethernet de 10 Mbps en banda base usando cable coaxial delgado de 50 Ω. 10Base2, el cual es parte de la especificación IEEE 802.3, tiene una distancia limite de 606.8 pies (185 metros) por segmento. Ver también *Cheapernet*, *EtherChannel*, *IEEE 802.3* y *Thinnet*.

**10Base5**
Especificación Ethernet de 10 Mbps usando cable coaxial de 50 Ω en banda base. 10Base5 el cual es parte de la especificación IEEE 802.3 de capa física en banda base, tiene una distancia límite de 1640 pies (500 metros) por segmento. Ver también *EtherChannel* e *IEEE 802.3*.

**10BaseT**
Especificación Ethernet de banda base a 10 Mbps usando dos pares de par trenzado (Categorías 3, 4 o 5): uno de los pares para transmitir datos y el otro para recibir datos. 10BaseT, el cual es parte de la especificación IEEE 802.3, tiene una distancia limite de aproximadamente 328 pies (100 metros) por segmento. Ver también *EtherChannel* e *IEEE 802.3*.

**100BaseFX**
Especificación en banda base de Fast Ethernet a 100 Mbps usando dos hilos de fibra óptica multimodo por link. Para garantizar la sincronización de la señal, un link 100BaseFX no puede exceder los 1312 pies (400 metros) de longitud. Basado en el estándar IEEE 802.3. Ver también *100BaseX*, *Fast Ethernet* e *IEEE 802.3*.

**100BaseT**
Especificación Ethernet de banda base a 100 Mbps usando cableado UTP. Como en la tecnología 10BaseT en la que esta basada, 100BaseT envía pulsos de enlace sobre el segmento de red cuando no hay trafico presente. De cualquier modo, estos pulsos de enlace contienen más información que aquellos usados en 10BaseT. Basado en el estándar IEEE 802.3. Ver también *10BaseT*, *Fast Ethernet* e *IEEE 802.3*.

**100BaseT4**
Especificación Ethernet de banda base a 100 Mbps usando cuatro pares de cables UTP de Categorías 3, 4 o 5. Para asegurar el correcto timing de señal, un segmento de 100BaseT4 no puede exceder los 328 pies (100 metros) de longitud. Basado en el estándar IEEE 802.3. Ver también *Fast Ethernet* e *IEEE 802.3*.

**100BaseTX**
Especificación Ethernet de banda base a 100 Mbps utilizando dos pares o de cableado UTP o STP. Los primeros pares de cables reciben los datos, los segundos transmiten datos. Para garantizar el timing correcto de señal, un segmento 100BaseTX no puede exceder los 328 pies (100 metros) de longitud. Basado en el estándar IEEE 802.3. Ver también *100BaseX*, *Fast Ethernet* e *IEEE 802.3*.

**100BaseX**
Especificación Ethernet de banda base a 100 Mbps que se refiere a los estándares 100BaseFX y 100BaseTX para Fast Ethernet sobre cableado de fibra óptica. Basado en el estándar IEEE 802.3. Ver también *100BaseFX*, *100BaseTX*, *Fast Ethernet* e *IEEE 802.3*.

**1000BaseF**
Un estándar IEEE para LANs Ethernet a 1 Gbps.

**802.x**
Set de estándares IEEE para la definición de los protocolos LAN.

## *A*

**Access Method – Método de Acceso**
Generalmente, la via en la cual dispositivos de red acceden al medio de red.

**ACK – Acknowlegdement**
Reconocimiento. Notificación de envío desde un dispositivo de red a otro para dar a conocer que algunos eventos han ocurrido (por ejemplo, la recepción de un mensaje). Algunas veces abreviado ACK.

**Address - Dirección**
Estructura de datos o convención lógica usada para identificar a una sola entidad, como un proceso particular o un dispositivo de red.

**Address Mapping – Mapeo de direcciones**
Una técnica que permite a diferentes protocolos interoperar trasladando direcciones de un formato a otro. Por ejemplo, cuando se rutea IP sobre X.25, las direcciones IP deben ser mapeadas a las direcciones X.25 y así los paquetes IP pueden ser transmitidos por la red X.25. Ver también *Address Resolution*.

**Address Resolution – Resolución de direcciones**
Generalmente, un método para resolver las diferencias entre esquemas de direcciones en computadoras. La Resolución de direcciones usualmente especifica un método para mapear las direcciones de la Capa de Red (Capa 3) a direcciones de la Capa de enlace de datos (Capa 2).

**Administrator – Administrador**
La persona quien indaga en el Registro de Usuarios para analizar el status individual de los suscriptores y problemas para generar estadísticas agregadas.

**Algorithm – Algoritmo**
Regla bien definida o proceso para llegar a la solución de un problema. En redes, los algoritmos usualmente se usan para determinar la mejor ruta de tráfico de una fuente o un destino particular.

**Alignment error – Error de alineamiento**
En las redes IEEE 802.3, es un error que ocurre cuando el número total de bits de una trama recibida no es divisible entre ocho. Los errores de alineamiento usualmente son causados por daño de tramas debido a colisiones.

**Analog Signal – Señal Análoga**
La representación de información como una cantidad física variable continuamente. Debido a que constantemente esta cambiando el valor de la onda en un punto dado del tiempo y el espacio, una señal análoga puede tener un número infinito de estados o valores. Esto contrasta con una señal digital que es expresada como una onda cuadrada y por lo tanto tiene un número muy limitado de estados discretos.

**Analog Transmission – Transmisión Análoga**
Señal de transmisión sobre cables o a través del aire en la cual información es transportada a través de la variación de alguna combinación de señal de amplitud, frecuencia y fase.

**ANSI – American National Standards Institute**
Instituto Nacional Americano de Estándares. Una organización voluntaria compuesta por miembros corporativos, de gobierno y otros que coordinan actividades relacionadas a aprobación de estándares, y posiciones de desarrollo para los Estados Unidos en organizaciones internacionales de estandarización. ANSI ayuda al desarrollo internacional y entre otras cosas, comunicaciones y redes. ANSI es miembro de la IEC y la ISO. Ver también *IEC* e *ISO*.

**Antena**
Un dispositivo para transmisión o recepción de radio frecuencia (RF). Las antenas se diseñan en específicas y relativamente bien definidas frecuencias.

**Aplicación**
Un programa que brinda una función directamente a un usuario. Los clientes FTP y Telnet son ejemplos de aplicaciones de red.

**Application Layer – Capa de aplicación**
Capa 7 del Modelo de Referencia OSI. Esta capa provee servicios a procesos de aplicación (como e-mail, transferencia de datos y emulación de terminal) que están fuera del modelo OSI.
La Capa de Aplicación identifica y establece la disponibilidad de conexión entre dos dispositivos (y los recursos requeridos para conectarlos), sincroniza aplicaciones cooperativas y establece un acuerdo en los procedimientos de recuperación de error y el control de la integridad de datos. Ver también *Data Link Layer*, *Network Layer*, *Physical Layer*, *Presentation Layer*, *Session Layer* y *Transport Layer*.

**ARPA – Advanced Research Projects Agency**
Agencia de Proyectos de Investigación Avanzados. Organización de investigación y desarrollo que es parte de DoD (Departamento de Defensa). ARPA es responsable de numerosos avances tecnológicos en comunicaciones y redes, ARPA evoluciono a DARPA y entonces regreso a ARPA de nuevo en 1994.

**ARPANET – Advanced Research Projects Agency Network**
Red de la Agencia de Proyectos de Investigación Avanzados (ARPA). Red de señal de paquetes switcheados establecida en 1969. ARPANET fue desarrollada en los 70's por BBN y fundada por ARPA (y después DARPA). Esta eventualmente evoluciono como la Internet. El termino ARPANET fue retirado oficialmente en 1990. Ver también *ARPA*.

**ASCII – American Standard Code for Information Interchange**
Código de 8 bits para representación de caracteres (7 bits mas paridad).

**Asynchronous transmission – Transmisión asíncrona**
Termino que describe las señales digitales que son transmitidas sin una medición de tiempo precisa. Como las señales generalmente tienen diferentes frecuencias y relaciones de fase diferentes, las transmisiones asíncronas usualmente encapsulan caracteres individuales en bits de control (llamados bits de inicio y parada) que designan el comienzo y el fin de cada carácter. Comparar con *Isochronous Transmission* y *Synchronous Transmission*.

**Atenuación**
Perdida de energía en la señal de comunicación.

**Autenticación**
En seguridad, la verificación de la identidad de una persona o proceso.

**Autorización**
El método para control de acceso remoto, incluyendo autorización completa o para cada servicio, por lista de cuenta de usuario y perfil, usuario de grupo de soporte y soporte para IP, IPX, ARA y Telnet.

**Availability – Disponibilidad**
El monto de tiempo que un sistema telefónico u otro dispositivo es operacional. La disponibilidad es representada como el radio del tiempo total que un dispositivo es operacional durante un intervalo de tiempo dado a lo largo de ese intervalo. Comparar con *Reliability* (Confiabilidad).

**Average rate – Tasa promedio**
Tasa promedio en kilobits por segundo (Kbps) en la cual un circuito virtual dado puede transmitir.

## *B*

**Backbone – Columna vertebral**
Parte de una red que actúa como la trayectoria primaria para el trafico que siempre es generado desde y destinado para otras redes.

**Bandwidth – Ancho de banda**
La diferencia entre las frecuencias más altas y más bajas disponibles para señales de red. El término también es usado para describir la capacidad de tasa del throughput de un medio de red dado o protocolo. El rango de frecuencias necesario para transportar una señal medida en Hertz (Hz).

**Bandwidth reservation – Ancho de banda reservado**
El proceso de asignar ancho de banda a usuarios y aplicaciones reservados por una red. Involucra la asignación de prioridades a diferentes flujos de tráfico basada en que tan críticos y sensibles al retardo son. Esto hace el mejor uso del ancho de banda y si la red esta congestionada, el tráfico de baja prioridad puede ser detenido.

**Baseband – Banda base**
Característica de una tecnología de red donde solo una frecuencia portadora es usada. Ethernet es un ejemplo de red de banda base. Contrasta con *Broadband*.

**Baudio**
Unidad de velocidad de señalización igual al número de elementos de señal discretos transmitidos por segundo. Baudio es sinónimo de los bits por segundo (bps) si cada elemento de señal representa exactamente 1 bit.

**BER**
**1.** Bit Error Rate (Tasa de Error de Bits). Radio de bits recibidos que contienen errores.
**2.** Basic Encoding Rules (Reglas Básicas de Codificación). Reglas para codificar unidades de datos descritas en el estándar ISO ASN.1.

**Binario**
Sistema de numeración caracterizado por unos y ceros (1=on, 0=off).

**Bit**
Digito binario usado en el sistema de numeración binario. Puede ser 1 o 0.

**Bit rate – Tasa de bits**
Velocidad en la cual los bits son transmitidos, usualmente expresada en bits por segundo (bps).

**Bluetooth**
Nombre común de la especificación industrial IEEE 802.15.1, que define un estándar global de comunicación inalámbrica que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia segura, globalmente y sin licencia de corto rango. Los principales objetivos que se pretende conseguir con esta norma son:
**1.** Facilitar las comunicaciones entre equipos móviles y fijos.
**2.** Eliminar cables y conectores entre éstos.
**3.** Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre nuestros equipos personales.
La especificación de Bluetooth define un canal de comunicación de máximo 720 Kb/s (1 Mbps de capacidad bruta) con rango óptimo de 10 metros (opcionalmente 100 m con repetidores). La frecuencia de radio con la que trabaja está en el rango de 2,4 a 2,48 GHz con amplio espectro y saltos de frecuencia con posibilidad de transmitir en full-duplex con un máximo de 1600 saltos/s. Los saltos de frecuencia se dan entre un total de 79 frecuencias con intervalos de 1MHz; esto permite dar seguridad y robustez. La potencia de salida para transmitir a una distancia máxima de 10 metros es de 0 dBm (1 mW), mientras que la versión de largo alcance transmite entre 20 y 30 dBm (entre 100 mW y 1 W).

**Bridge – Puente**
Dispositivo que conecta y pasa paquetes entre dos segmentos de red que utilizan el mismo protocolo de comunicaciones. Los bridges o puentes operan en la Capa de Enlace de datos (Capa 2) del modelo de referencia OSI. En general un puente filtra, reenvía o inunda una trama entrante basada en la dirección MAC de esa trama. Ver también *Relay*.

**Broadband – Banda ancha**
**1.** Sistema de transmisión que multiplexa múltiples señales independientes en un solo cable.
**2.** Terminología de telecomunicaciones: Cualquier canal teniendo un ancho de banda mayor que un canal de voz (4 KHz).
**3.** Terminología LAN: Un cable coaxial en el cual señales análogas son usadas. Un sistema RF con una tasa constante de datos de o arriba de 1.5 Mbps. También llamado *Wideband*. Contrasta con banda base.

**Broadcast**
Paquetes de datos que son enviados a todos los nodos en una red. Los broadcasts son identificados por una dirección broadcast. Comparar con *Multicast* y *Unicast*.

**Broadcast address – Dirección broadcast**
Una dirección especial reservada para enviar un mensaje a todas las estaciones. Generalmente, una dirección broadcast es una dirección de destino MAC de todas las estaciones.

**Buffer**
Area de almacenamiento usada para manejar datos en transito. Los buffers son usados en las redes para compensar diferencias en la velocidad de procesamiento entre dispositivos de red. Ráfagas de datos pueden ser almacenadas en buffers hasta que puedan ser manejados por dispositivos de procesamiento más lentos.

**Burst – Ráfaga**
En comunicaciones de datos, una secuencia de señales contadas como una unidad de acuerdo con algún criterio especifico o medida.

**Bus**
Trayectoria de una señal física común compuesta por cables u otro medio a través del cual las señales pueden ser enviadas desde una computadora a otra.

**Bus topology – Topología de bus**
Arquitectura lineal LAN en la cual las transmisiones desde las estaciones de la red se propagan a lo largo del medio y son recibidas por todas las estaciones. Comparar con *Topología en anillo* y *Topología de árbol*.

**Byte**
Termino utilizado para referirse a una serie de dígitos binarios consecutivos que son operados como una unidad (por ejemplo un byte de 8 bits).

## *C*

**Cable**
Medio de transmisión de cable de cobre o fibra óptica envuelto en una cubierta protectora.

**Carrier – Portadora**
Una onda electromagnética o de corriente alterna de una frecuencia sencilla, adecuada para modularla por otra señal de datos sostenida. Ver también *Modulación*.

**Carrier Detect – Detección de Portadora**
Una señal que indica si una interfaz esta activa.

**CDDI – Interfaz de Datos Distribuida de Cobre**
La implementación de protocolos FDDI sobre cableado STP y UTP. CDDI opera sobre relativamente pequeñas distancias (cerca de 100 yardas, 100 metros), dando tasas de datos de 100 Mbps usando una arquitectura de anillo doble proveyendo redundancia. Comparar con *FDDI*.

**CENELEC**
Comité Europeo de Normalización Electrotécnica. CENELEC es el comité europeo para estandarización electrotécnica. Puesto en marcha en 1973 y fue oficialmente reconocido como la Organización de Estándares Europeos en su campo por la Comisión Europea Directiva. CENELEC trabaja con 40,000 expertos técnicos en todos los países para publicar estándares para el mercado europeo.

**Channel – Canal**
**1.** Trayectoria de comunicación suficientemente amplia para permitir una transmisión de RF sencilla. Canales múltiples pueden ser multiplexados sobre un solo cable en ciertos entornos.
**2.** En IBM, el camino especifico entre grandes computadoras (como los mainframes) y dispositivos periféricos agregados.
**3.** Asignación de una frecuencia específica y ancho de banda. Los canales que son usados para televisión en los Estados Unidos son de 6 MHz de ancho.

**Checksum**
Método para checar la integridad de los datos transmitidos. Un checksum es un valor entero computado desde una secuencia de octetos tomados a través de una serie de operaciones aritméticas. El valor es recomputado al receptor terminal y es comparado para verificación.

**Cliente**
Nodo o programa de software que solicita servicios desde un servidor.

**Cliente/Servidor**
Termino usado para describir el procesamiento distribuido en sistemas de red en los cuales las responsabilidades de transacción están divididos en dos partes: cliente y servidor. Ambos términos (cliente y servidor) pueden ser aplicados a programas de software o a dispositivos.

**Coaxial cable – Cable coaxial**
Cable que consiste en una malla de conductor externa que rodea a un conductor aislado. Dos tipos de cable coaxial se utilizan en las LAN: cable de 50 Ohms el cual se usa en señales digitales y el cable de 75 Ohms el cual se usa para señales análogas y señales digitales de alta velocidad.

**Codificación**
Técnicas eléctricas usadas para convertir señales binarias.

**Colisión**
En Ethernet, el resultado de la transmisión simultanea de dos nodos. Las tramas de cada dispositivo impactan y son dañadas cuando se encuentran en un medio físico. Ver también *Dominio de colisión*.

**Collision Domain – Dominio de colisión**
En Ethernet, el área de red dentro de la cual las tramas colisionan y son propagadas. Los repetidores y los hubs propagan colisiones; los switches LAN, bridges y ruteadores no.

**CRC – Cyclic Redundancy Check**
Chequeo de Redundancia Cíclica. Técnica de chequeo de error en la cual la trama recibida calcula un residuo dividiendo el contenido de una trama por un divisor primo binario y comparando el residuo calculado con el valor almacenado en la trama por el nodo emisor.

**Cross-talk**
Interferencia en la transferencia de energía de un circuito a otro.

**Cryptographic Algorithm – Algoritmo criptográfico**
Algoritmo que emplea la ciencia de la Criptografía, incluyendo algoritmos de encriptación, algoritmos de señal digital, etc.

**CSMA/CD – Carrier Sense Multiple Access/Collision Detect**
Mecanismo de acceso al medio donde los dispositivos listos a transmitir datos primero checan el canal para una portadora. Si no se detecta portadora para un periodo especifico de tiempo, un dispositivo puede transmitir. Si dos dispositivos transmiten al mismo tiempo, una colisión ocurre y es detectada por todos los dispositivos que colisionaron. Esta colisión subsecuentemente retarda retransmisiones desde aquellos dispositivos por algún largo de tiempo aleatorio. Ethernet e IEEE 802.3 usan el acceso CSMA/CD.

## *D*

**Dark Fiber – Fibra negra**
Cable de fibra óptica sin uso. Cuando esta llevando una señal, es llamado lit fiber.

**Datagrama**
Agrupación lógica de información enviada como una unidad de capa de red sobre un medio de transmisión sin establecimiento previo de un circuito virtual. Los datagramas IP son las unidades de información primarias en la Internet.

**Datalink layer – Capa de enlace de datos**
Capa 2 del modelo de referencia OSI. Provee transito confiable de datos a través de un medio físico. La capa de enlace de datos es concerniente con la dirección física, topología de red, error de notificación, entrega ordenada de tramas y control de flujo. El IEEE divide esta capa en dos subcapas: la subcapa MAC y la subcapa LLC.

**dB – Decibeles**
Unidad para la medición de radios de potencia relativos en términos de ganancia o pérdida. Las unidades son expresadas en términos del logaritmo de base 10 de un radio y típicamente se expresan en Watts.
Los dB no son valores absolutos, si es esta una medición de perdida o ganancia de potencia entre dos dispositivos.

**Delay – Retardo**
El tiempo entre el inicio de una transacción de un emisor y la primera respuesta recibida por el emisor. También, el tiempo requerido para mover un paquete desde una fuente a un destino sobre una trayectoria dada.

**Demodulation – Demodulación**
Proceso de regresar una señal modulada a su forma original. Los módems realizan la demodulación tomando una señal análoga y regresándola a su forma original (digital). Ver también *Modulación*.

**Destination address – Dirección destino**
Dirección de un dispositivo de red que esta recibiendo datos. Ver también *Dirección fuente*.

**DIN – Deutsche Industrie Norm**
Organización de Estándares Nacionales de Alemania.

**Domain – Dominio**
En seguridad, un entorno o contexto que es definido por una política de seguridad, un modelo de seguridad o una arquitectura de seguridad para incluir un set de recursos de sistema y el set de entidades de sistema que tienen el acceso correcto a los recursos.

## *E*

**Electromagnetic Interference – EMI**
Interferencia Electromagnética. Interferencia por señales electromagnéticas que pueden causar reducción de la integridad de datos e incrementar tasas de error en canales de transmisión.

**Electromagnetic Pulse – EMP**
Pulso Electromagnético. Causado por la luz u otro fenómeno de alta energía. Capaz de acoplar suficiente energía en conductores no blindados como para destruir dispositivos electrónicos.

**Encapsulación**
Envoltura de datos en una cabecera de un protocolo particular. Por ejemplo, los datos Ethernet son envueltos en una cabecera Ethernet específica antes de transitar en la red.

**Encoder – Codificador**
Dispositivo que modifica información en el formato de transmisión requerido.

**Encryption – Encriptación**
Aplicación de un algoritmo especifico a datos para alterar la apariencia de los mismos haciendo estos incomprensibles a aquellos quienes no están autorizados a ver esta información. Ver también *Decryption*.

**Enterprise Network – Red empresarial**
Red grande y diversa que conecta la mayoría de puntos en una compañía u otra organización. Difiere de la WAN en que es manejada y mantenida de forma privada.

**ERP – Enterprise Resource Planning**
Sistema de Planeación de Recursos Empresariales. Sistemas integrados (o en los que se pretenden integrar) todos los datos y procesos de una organización a un sistema unificado. Un sistema ERP típico usara múltiples componentes de software y hardware de computadora para ejecutar la integración. Un ingrediente clave en la mayoría de los sistemas ERP es el uso de una base de datos para almacenar los datos de los diversos módulos del sistema.

**Ethernet**
Especificación LAN en banda base inventada en Xerox Corporation y desarrollada por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet usan el método de acceso CSMA/CD y corren sobre una gran variedad de tipos de cable desde los 10 Mbps.

## *F*

**Fast Ethernet**
Cualquiera de las especificaciones Ethernet a 100 Mbps. Fast Ethernet ofrece un incremento de velocidad de 10 veces con respecto a la especificación Ethernet 10BaseT mientras se preservan cualidades como el formato de trama, mecanismos MAC y MTU.
Con estas similitudes se permite el uso de aplicaciones existentes 10BaseT y herramientas de administración de red en las redes Fast Ethernet. Basada en una extensión de la especificación IEEE 802.3.

**FCS – Frame Check Sequence**
Secuencia de chequeo de trama. Caracteres extra sumados a una trama para propósitos de control de errores. Usado en Ethernet, HDLC, Frame Relay y otros protocolos de enlace de datos.

**FDDI – Fiber Distributed Data Interface**
Estándar LAN, definido por el ANSI X3T9.5, especificando una red token ring a 100 Mbps utilizando cable de fibra óptica con distancias de transmisión de hasta 2 Km. FDDI usa una arquitectura de doble anillo para proveer redundancia.

**Fibra óptica**
Método y medio para la transmisión de información (audio, video, datos). La luz es modulada y transmitida sobre fibras de vidrio de alta pureza tan delgadas como un cabello. La capacidad de ancho de banda de un cable de fibra óptica y las tasas de datos que puede manejar son mucho mas grandes que las del cable de cobre convencional. La fibra óptica es más cara pero no es susceptible a interferencia electromagnética.

**Firewall**
Router o servidor de acceso diseñado como un buffer entre cualquier red publica conectado a una red privada. Un firewall usa listas de acceso y otros métodos para no comprometer la seguridad de la red privada.

**Frame – Trama**
Agrupación lógica de información enviada como una unidad de capa de enlace de datos sobre un medio de transmisión. Siempre se refiere a la cabecera y al final de la unidad, usados para la sincronización y el control de errores que rodean los datos de usuario contenidos en la unidad. Los términos célula, datagrama, mensaje, paquete y segmento también son usados para describir agrupaciones lógicas de información en varias capas del modelo de referencia OSI y en varios círculos de tecnologías.

**Full Duplex**
Capacidad de transmisión de datos simultáneos entre una estación emisora y una receptora. Comparar con *Half duplex* y *Simplex*.

## *G*

**Gb - Gigabit**
Aproximadamente 1, 000, 000,000 de bits.

**GB - Gigabyte**
Aproximadamente 1, 000, 000,000 de bytes.

**Gbps**
Gigabits por segundo.

**GBps**
Gigabytes por segundo.

**Gigabit Ethernet**
Estándar para una red Ethernet de alta velocidad, aprobado por el comité IEEE de estándares 802.3z en 1996.

**GSM – Global System for Mobile Communication**
Un estándar de red inalámbrica móvil de segunda generación de segunda generación (2G) definido por el ETSI, GSM es desarrollado ampliamente a través del mundo. GSM usa tecnología TDMA y opera en la banda de radio de 900 MHz.

## *H*

**Half duplex**
Capacidad para transmisión de datos en una sola dirección a un tiempo entre una estación emisora y una receptora.

**Handshake – Saludo**
Secuencia de mensajes intercambiados entre dos o mas dispositivos de red para asegurar la sincronización de la transmisión.

**Header – Cabecera**
Información de control situada antes de los datos cuando se encapsulan esos datos para una transmisión de red.

**Host – Huésped**
Computadora dentro de una red. Similar a un nodo, excepto que el host usualmente implica una computadora, donde los nodos generalmente aplican a un sistema de red, incluyendo servidores de acceso y routers. Ver también *Nodo*.

**Hub – Concentrador**
**1.** Termino usado para describir un dispositivo que sirve como centro de una red de topología en estrella.
**2.** Dispositivo de hardware o software que contiene múltiples módulos de red independientes pero conectados a equipo de red. Los hubs pueden ser activos (donde ellos repiten las señales que enviadas a través de ellos) o pasivos (donde no repiten, solo separan las señales enviadas a través de ellos).
**3.** En Ethernet e IEEE 802.3, un repetidor Ethernet multipuerto.

## *I*

**IEC 61508**
Estándar titulado "Seguridad funcional de sistemas eléctricos/electrónicos/programables relacionados a la seguridad" (E/E/PES); esta intentando ser un estándar de seguridad funcional básico aplicable a todos los tipos de industria. IEC 61508 define la seguridad funcional como "parte de toda la seguridad relacionada al EUC (Equipment Under Control, Equipo bajo control) y el sistema de control del EUC el cual depende del correcto funcionamiento de los sistemas E/E/PES relacionados a la seguridad, otras tecnologías de sistemas relacionados a la seguridad y las instalaciones externas para reducción de riesgos.
El estándar cubre el ciclo de vida de seguridad completo y puede necesitar interpretación para desarrollar estándares específicos en cada sector. El ciclo de vida de seguridad tiene 16 fases que se dividen en 3 grupos: fases 1-5 dirección de análisis, fases 6-13 dirección de realización y fases 14-16 dirección de operación.
El estándar IEC 61508 define los siguientes puntos acerca de los riesgos:

- Un riesgo de cero nunca puede ser conseguido
- La seguridad debe ser considerada desde el inicio
- Riesgos no tolerables deben ser reducidos

**IEC – International Electrotechnical Comission**
Comisión Electrotécnica Internacional. Grupo industrial que escribe y distribuye estándares para productos eléctricos y componentes.

**IEEE – Institute of Electrical and Electronics Engineers**
Organización profesional la cual dentro de sus actividades incluye el desarrollo de estándares de red y comunicaciones. Los estándares IEEE para LAN son los estándares predominantes hoy en día.

**Interface – Interfaz**
**1.** Conexión entre dos sistemas o dispositivos.
**2.** En terminología de ruteo, una conexión de red.
**3.** En telefonía, una frontera compartida definida por características de interconexión físicas comunes, señales características y significados de señales intercambiadas.
**4.** Frontera entre capas adyacentes del modelo de referencia OSI.

**Interoperabilidad**
Capacidad del equipo computacional fabricado por diferentes vendedores de comunicarse con otros exitosamente dentro de una red.

**ISO – International Organization for Standardization**
Organización internacional que es responsable de un amplio rango de estándares, incluyendo aquellos relevantes para el trabajo en redes. ISO desarrollo el modelo de referencia OSI.

**Isochronous transmission – Transmisión Isócrona**
Transmisión asíncrona sobre un enlace de datos síncrono. Las señales isócronas requieren una tasa de bits constante para transporte confiable. Comparar con *Asynchronous transmission*, *Plesiochronous transmission* y *Synchronous transmission*.

## *J*

**Jitter – Fluctuación**
**1.** La fluctuación del retardo entre paquetes; que es la diferencia entre el arribo y llegada de paquetes. La fluctuación es una medida de *QoS* importante para aplicaciones de video y voz.
**2.** Distorsión de línea en la comunicación analógica causada por la variación de una señal desde sus posiciones de referencia de tiempo. La fluctuación puede causar perdida de datos, especialmente a altas velocidades.

## *L*

**LAN – Local Area Network**
Red de datos de alta velocidad y pocos errores que cubre una relativamente pequeña área geográfica. Las LAN conectan estaciones de trabajo, periféricos y otros dispositivos en un edificio sencillo o en otra área limitada. Los estándares LAN especifican el cableado y señalización de las capas físicas y de enlace de datos del modelo OSI. Ethernet, FDDI y Token Ring usan ampliamente las tecnologías LAN.

**LAN switch – Switch LAN**
Switch de alta velocidad que reenvía paquetes entre segmentos de enlace de datos. La mayoría de switches LAN reenvían tráfico basado en las direcciones MAC.

**Latencia**
**1.** Retardo entre el tiempo que un dispositivo pide acceso a una red y el tiempo en que es garantizado su permiso para transmitir.
**2.** Retardo entre el tiempo que un dispositivo recibe una trama y el tiempo que la trama es reenviada hacia el puerto de destino.

**Link – Enlace**
Canal de comunicaciones de red consistente en un circuito o trayectoria de transmisión y todo el equipo relacionado entre un emisor y un receptor. El término es más utilizado para referirse a una conexión WAN. Algunas veces referido como una línea o enlace de transmisión.

**LLC – Logical Link Control**
La mas alta de las subcapas de la capa de enlace de datos definida por el IEEE. La subcapa LLC maneja control de errores, control de flujo, tramas y direccionamiento de subcapa MAC. El protocolo mas relevante es el IEEE 802.3, el cual incluye tanto variantes orientadas con conexión y sin conexión. Ver también *Data-Link Layer* y *MAC*.

## *M*

**MAC – Media Access Control**
Subcapa mas baja de la capa de enlace de datos definida por el IEEE. La subcapa MAC maneja el acceso al medio compartido

**MAC Address – Dirección MAC**
Dirección estandarizada de la capa de enlace de datos que es requerida para cada puerto o dispositivo que se conecta a una LAN. Otros dispositivos en la red usan estas direcciones para localizar puertos específicos en la red y crear y actualizar tablas de ruteo y estructuras de datos. Las direcciones MAC tienen 6 bytes de longitud y son controladas por el IEEE. También conocida como dirección de hardware, dirección de capa MAC y dirección física.

**Manchester Encoding – Codificación Manchester**
Esquema de codificación digital usado por el IEEE 802.3 y Ethernet en el cual una transición de tiempo de medio bit es usada como reloj y un 1 es denotado por un nivel alto durante la primera mitad del bit de tiempo.

**MAP – Manufacturing Automation Protocol**
Arquitectura de red creada por General Motors para cumplir las necesidades de especificación en las fábricas. El MAP especifica una LAN Token-pass similar a IEEE 802.4.

**Media**
Plural de medio. Varios entornos físicos a través de los cuales pasan las señales de transmisión. Media de red común incluye cable de par trenzado, coaxial, de fibra óptica y la atmosfera (a través de la cual las microondas, el laser y la transmisión infrarroja ocurren). Algunas veces llamado medio físico.

**MES – Manufacturing Execution System**
Sistema de Ejecución de Manufactura. Sistema que usan compañías para medir y controlar actividades criticas de producción. Algunos de los beneficios relacionados a las soluciones MES son el incremento de trazabilidad, productividad y calidad.

**Modulación**
Proceso en el cual las características de las señales eléctricas son transformadas para representar información. Los tipos de modulación incluyen el AM, FM y PAM.

**Multicast – Multidifusión**
Paquetes sencillos copiados por una red y enviados a un subset de direcciones de red. Estas direcciones son especificadas en el Destination Address Field (campo de destino de dirección). Comparar con *Broadcast* y *Unicast*.

**Multicast address – Dirección de Multidifusión**
Dirección sencilla que se refiere a múltiples dispositivos de red. Sinónimo de grupo de direcciones.

## *N*

**Network – Red**
Colección de computadoras, impresoras, routers, switches y otros dispositivos que pueden comunicarse entre si sobre un medio de transmisión.

**Network Layer – Capa de Red**
Capa 3 del modelo de referencia OSI. Esta capa provee conectividad y selección de trayectoria entre dos dispositivos terminales. La capa de red es la capa en la cual ocurre el ruteo. Ver también *Application Layer*, *Datalink Layer*, *Physical Layer*, *Presentation Layer*, *Session Layer* y *Transport Layer*.

**NIC – Network Interface Card**
Tarjeta que proporciona capacidades de comunicación de red a y desde una computadora.

**Nodo**
Punto final de una conexión de red o unión común de dos o más líneas en una red. Los nodos pueden ser procesadores, controladores, cables, fibras, etc.

## *O*

**Open architecture – Arquitectura abierta**
Arquitectura en la que desarrolladores legalmente pueden desarrollar productos para los cuales las especificaciones son del dominio publico.

**OSI – Open System Interconnection**
Programa internacional de estandarización creado por la ISO y la ITU-T para desarrollar estándares redes de datos que facilitaran la interoperabilidad de equipo de múltiples fabricantes.

**OSI reference model – Modelo de referencia OSI**
Modelo de arquitectura de red desarrollado por la ISO y la ITU-T. El modelo consiste en siete capas, cada una especifica funciones de red particulares como direccionamiento, control de flujo, control de errores, encapsulación y transferencia de mensaje correcta. La capa más baja (Capa física) esta más cerca al medio físico.
Las dos primeras capas son implementadas en hardware y software y las cinco capas de más arriba solo son implementadas en software. El modelo de referencia OSI es utilizado universalmente para enseñar y entender la funcionalidad de red. Ver también *Application Layer*, *Datalink Layer*, *Network Layer*, *Physical Layer*, *Presentation Layer*, *Session Layer* y *Transport Layer*.

## *P*

**Packet – Paquete**
Agrupación lógica de información que incluye una cabecera que contiene información de control y usualmente datos de usuario. Los paquetes son siempre más utilizados para referirse a unidades de datos de capas de red. Los términos datagrama, trama, mensaje y segmento también son usados para describir grupos de información lógica en varias capas del modelo de referencia OSI.

**Physical Layer – Capa física**
Capa 1 del modelo de referencia OSI. La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre dos dispositivos terminales. Ver también *Application Layer*, *Datalink Layer*, *Network Layer*, *Presentation Layer*, *Session Layer* y *Transport Layer*.

**Plesiochronous transmission – Transmisión plesiocrona**
Termino que describe las señales digitales que son generadas desde diferentes relojes de comparable exactitud y estabilidad. Comparar con *Transmisión asíncrona*, *isócrona* y *síncrona*.

**Polling – Poleo**
Método de acceso en el cual un dispositivo de red primario verifica, en un estilo ordenado, si los dispositivos secundarios tienen datos para transmitir. La verificación ocurre en forma de un mensaje a cada secundario que da al secundario el derecho a que transmita.

**Port – Puerto**
Interfaz de un dispositivo de red (como un router).

**Presentation Layer – Capa de Presentación**
Capa 6 del modelo de referencia OSI. Esta capa asegura que la información enviada por la capa de aplicación en un sistema sea legible por la capa de aplicación de otro dispositivo. A la capa de presentación le conciernen también las estructuras de datos usadas por programas y por lo tanto negocia la sintaxis de transferencia de datos para la capa de aplicación. Ver también *Application layer*, *Datalink Layer*, *Network Layer*, *Physical Layer*, *Session Layer* y *Transport Layer*.

**Propagation Delay – Retardo de propagación**
Tiempo requerido para que los datos viajen sobre una red desde su fuente a su último destino.

**Protocol Stack – Pila de protocolo**
Set de protocolos de comunicaciones relacionados que operan juntos y como un grupo, direcciona comunicación a algunas o a las siete capas del modelo de referencia OSI. No siempre la pila del protocolo cubre cada capa del modelo, y siempre un protocolo simple en la pila direcciona un número de capas al mismo tiempo. TCP/IP es una pila de protocolo típica.

## *Q*

**QoS – Quality of Service**
Calidad de servicio. Medida de rendimiento para un sistema de transmisión que refleja su calidad de transmisión y disponibilidad de servicio.

**Query – Pregunta, duda**
Mensaje usado para averiguar acerca del valor de algunas variables o set de variables.

**Queue**
**1.** Generalmente, una lista ordenada de elementos esperando a ser procesados.
**2.** En ruteo, un grupo de paquetes esperando a ser reenviados sobre un router.

**Queuing delay**
Monto de tiempo que deben esperar los datos antes de que puedan ser transmitidos en un circuito físico estadísticamente multiplexado.

## *R*

**Redundancy – Redundancia**
En redes, la duplicación de dispositivos, servicios o conexiones que en un evento de falla, los dispositivos redundantes, servicios o conexiones pueden ejecutar el trabajo de eso que fallo. Ver también *Redundant System*.

**Redundant system – Sistema redundante**
Computadora, router, switch u otro sistema que contiene dos o más de los subsistemas más importantes, como son dos trayectorias, dos procesadores, dos fuentes de poder, etc.

**Repeater – Repetidor**
Dispositivo que regenera y propaga señales eléctricas entre dos segmentos de red.

**Ring topology – Topología de anillo**
Topología de red que consiste en una serie de repetidores conectados a otro por enlaces de transmisión direccional para formar un bucle cerrado sencillo. Cada estación en la red se conecta a la red con un repetidor. Aunque lógicamente es un anillo, las topologías de anillo la mayoría de las veces están organizadas en un bucle cerrado en estrella. Comparar con *Bus topology*, *Star topology* y *Tree topology*.

**Router – Ruteador**
Dispositivo de capa de red que usa una o mas medidas para determinar el camino óptimo mediante el cual el tráfico de red debería ser reenviado. Los routers reenvían paquetes de una red a otra basados en la información de la capa de red. Ocasionalmente llamados Gateways (aunque la definición de gateway esta fuera de moda).

**Routing- Ruteo**
Proceso de encontrar una trayectoria a un dispositivo de destino.

## *S*

**SDH – Synchronous Digital Hierarchy**
Jerarquía Digital Síncrona. Estándar europeo que define sets de tasas y formatos estándar que son transmitidos usando señales ópticas sobre fibra. SDH es similar a SONET, con una tasa básica SDH de 155.52 Mbps, designado como STM-1. Ver también *SONET*.

**Segmento**
**1.** Sección de una red que esta limitada por puentes (bridges), routers (ruteadores) o switches (interruptores).
**2.** En una LAN usando topología de bus, un segmento es un circuito eléctrico continuo que siempre esta conectado a otros segmentos con repetidores.
**3.** Termino usado en la especificación TCP para describir una unidad sencilla de la capa de transporte de información.
Los términos datagram (datagrama), frame (trama), message (mensaje) y packet (paquete) también son utilizados para describir agrupaciones lógicas de información de varias capas del modelo de referencia OSI y en varios círculos de tecnologías.

**Session Layer – Capa de sesión**
Capa 5 del modelo de referencia OSI. Esta capa establece, maneja y termina sesiones entre aplicaciones y administra el intercambio de datos entre entidades de la capa de presentación. Ver también *Application Layer*, *Datalink Layer*, *Network Layer*, *Physical Layer* y *Presentation Layer*.

**Shielded cable – Cable blindado**
Cable que tiene una capa de blindaje de aislamiento para reducir las EMI.

**Shielded twisted-pair – STP**
Par trenzado blindado. Cableado de 2 pares de cables que se usan en implementaciones de red. El cable STP tiene un aislamiento de blindaje para reducir las EMI. Comparar con *UTP*.

**SIL – Safety Integrity Level**
Nivel de seguridad integrada. SIL es una representación estadística de la confiabilidad de un SIS (Sistema Integrado de Seguridad) cuando un proceso en demanda ocurre. Este es usado en los estándares ANSI/ISA-S84.01 e IEC 61508 para medir la confiablidad del SIS. Existen tres categorías de SIL: SIL's 1, 2 y 3.

IEC incluye un nivel 4 que ISA no. El sistema más efectivo o confiable es el que tiene nivel SIL más alto. El SIL esta relacionado con la probabilidad de falla en demanda (PFD), lo cual es equivalente a la no disponibilidad de un sistema al tiempo de un proceso en demanda.

**Simplex**
Capacidad de transmisión en una sola dirección entre una estación emisora y una receptora. La televisión de difusión es un ejemplo de la tecnología simplex. Comparar con *full duplex* y *half duplex*.

**SONET – Synchronous Optical Network**
-Red Óptica Síncrona. Un formato estándar para transportar un amplio rango de servicios de telecomunicaciones digitales sobre fibra óptica. SONET esta caracterizado por tasas de línea estándar, interfaces ópticas y formatos de señal.
-Especificación de red de alta velocidad síncrona (hasta 2.5 Gbps) desarrollada por Bellcore y diseñada para trabajar sobre fibra óptica. STS-1 es el bloque de construcción básico de SONET. Aprobado como estándar internacional en 1988. Ver también *SDH*.

**Source address – Dirección fuente**
Dirección de un dispositivo de red que esta mandando datos. Ver también *Destination address*.

**Standard – Estándar**
Set de reglas o procedimientos que o son ampliamente usados u oficialmente especificados.

**Star topology – Topología de estrella**
Topología LAN en la cual los puntos terminales en una red están conectados a un switch central común por enlaces punto-a-punto. Una topología de anillo que es organizada como una estrella implementa una estrella de bucle cerrado unidireccional, en vez de enlaces punto-a-punto. Comparar con *topología de bus*, *topología de anillo* y *topología de árbol*.

**Subnetwork – Subred**
En redes IP, una red compartiendo una dirección de subred particular. Las subredes son redes arbitrariamente segmentadas por un administrador de red con la finalidad de dar una estructura de ruteo jerárquica y multinivel mientras se protege la subred del complejo direccionamiento de las redes agregadas. Algunas veces llamada Subnet.

**Switch – Interruptor**
Dispositivo de red que filtra, reenvía e inunda tramas basado en la dirección de destino de cada trama. El switch opera en la Capa de enlace de datos del modelo de referencia OSI.

**Synchronisation – Sincronización**
Establecimiento de un tiempo común entre un dispositivo emisor y uno receptor.

**Synchronous transmission – Transmisión síncrona**
Termino que escribe las señales digitales que son transmitidas con un clocking preciso. Como las señales tienen la misma frecuencia con caracteres individuales encapsulados en bits de control (llamados bits de inicio y bits de parada) que designan el inicio y el final de cada carácter. Comparar con *transmisión asíncrona*, *transmisión isócrona* y *transmisión plesiocrona*.

## *T*

**Tag – Etiqueta**
Información de identificación que incluye un número más otra información.

**TDR – Time Domain Reflectometer**
Reflectometro de dominio de tiempo. Dispositivo capaz de enviar señales a través de un medio de red para checar la continuidad del cable y otros atributos. Los TDRs son usados para encontrar problemas de red en la capa física.

**Topology – Topología**
Arreglo físico o lógico de nodos de red y cableado dentro de una red estructurada empresarial o industrial.

**Transport Layer – Capa de transporte**
Capa 4 del modelo de referencia OSI. Esta capa es la responsable de la comunicación de red confiable entre nodos terminales. La capa de transporte provee mecanismos para el establecimiento, mantenimiento y terminación de circuitos virtuales, detección de falla de transporte y recuperación e información de control de flujo. Ver también *capa de aplicación*, *capa de enlace de datos*, *capa de red*, *capa física* y *capa de sesión*.

**Tree topology – Topología de árbol**
Topología LAN similar a la topología de bus, excepto que las topologías de árbol pueden contener ramas con múltiples nodos. Las transmisiones desde una estación se propagan a lo largo del medio y son recibidas por todas las demás estaciones. Comparar con topología de bus, topología de anillo y topología de estrella.

## *U*

**Unicast**
Mensaje enviado a un destino sencillo de red.

**Unicast address – Dirección unicast**
Dirección que especifica un dispositivo de red simple. Comparar con *dirección broadcast* y *dirección multicast*.

## *Z*

**ZigBee**
Protocolo de comunicaciones inalámbrico similar a Bluetooth y basado en el estándar para redes inalámbricas de área personal (WPANs) IEEE 802.15.4. Principalmente, el ámbito en el que se usará será la domótica, debido a su bajo consumo, su sistema de comunicaciones vía radio (con topología MESH) y su fácil integración (se pueden fabricar nodos con muy poca electrónica).
ZigBee es muy similar al Bluetooth pero con algunas diferencias:
**1.** Una red ZigBee puede constar de un máximo de 64000 nodos, frente a los 8 máximos de una red Bluetooth.
**2.** Menor consumo eléctrico que el ya de por sí bajo del Bluetooth. En términos exactos, ZigBee tiene un consumo de 30 mA transmitiendo y de 3ma en reposo, frente a los 40ma transmitiendo y 0.2ma en reposo que tiene el Bluetooth. Este menor consumo se debe a que el sistema ZigBee se queda la mayor parte del tiempo dormido, mientras que en una comunicación Bluetooth esto no se puede dar, y siempre se está transmitiendo y/o recibiendo.
**3.** Tiene un ancho de banda de 250 Kbps, mientras que el Bluetooth tiene 1 Mbps.
**4.** Debido al ancho de banda de cada uno, uno es más apropiado que el otro para ciertas cosas. Por ejemplo, mientras que el Bluetooth se usa para aplicaciones como el Wireless USB, los teléfonos móviles y la informática casera, el ancho de banda del ZigBee se hace insuficiente para estas tareas, desviándolo a usos tales como la Domótica, los productos dependientes de la batería, los sensores médicos, y en artículos de juguetería, en los cuales la transferencia de datos es menor.
**5.** Existe una versión que integra el sistema de radiofrecuencias característico de Bluetooth junto a interfaz de transmisión de datos vía infrarroja desarrollado por IBM mediante un protocolo ADSI y MDSI.

# Bibliografía

**1. IAONA Handbook – Industrial Ethernet**
Industrial Automation Open Networking Alliance
2005, Tercera edición

**2. The IAONA Handbook for Network Security, Draft Version v0.4**
Industrial Automation Open Networking Alliance
2003

**3. Internetworking Technologies Handbook**
Cisco Systems
2003, Segunda edición

**4. Dictionary of Internetworking Terms and Acronyms**
Cisco Systems
2001, Tercera edición

# En la WEB

**1.** http://ethernet.industrial-networking.com/articles/technical.asp

**2.** http://ethernet.industrial-networking.com/articles/articles.asp

**3.** www.dyadem.com/engineering/risk_management/engineering_services/sil/index.htm

**4.** http://es.wikipedia.org/wiki/ZigBee

**5.** http://es.wikipedia.org/wiki/Bluetooth

**6.** http://en.wikipedia.org/wiki/Manufacturing_Execution_System

**7.** http://en.wikipedia.org/wiki/Management_information_system

**8.** http://en.wikipedia.org/wiki/Enterprise_resource_planning

**9.** http://en.wikipedia.org/wiki/IEC_61508

**10.** http://en.wikipedia.org/wiki/Safety_Integrity_Level