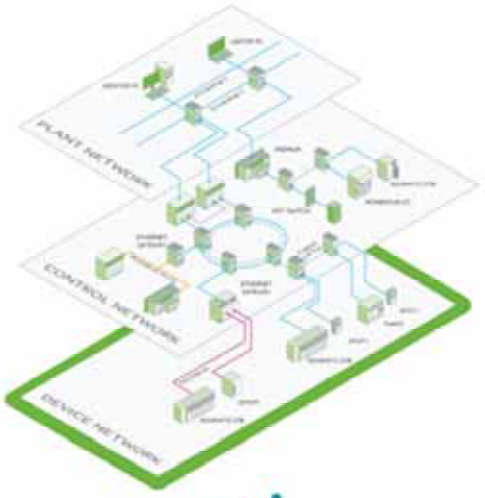
(N1) Introducción a las Aplicaciones Industriales del Procesamiento Digital de Datos

Redes Industriales

Prof. Ing. Diego M. Romero
Julio 2011



DEPARTAMENTO DE COMPUTACION

Programa

- Día 1:
  - Repaso de algunos conceptos sobre redes
  - Requerimientos de las redes Ethernet para aplicaciones industriales
  - Switches Ethernet para aplicaciones de piso de planta.
- Día 2
  - Protocolos de capa de aplicación sobre Ethernet de uso industrial
  - Conectividad inalámbrica en ámbitos industriales
  - Conversores Serie a Ethernet
  - Conversores de medio físico
- Día 3
  - Generalidades de un sistema de Interfaz Humano-Máquina (HMI)
  - La Base de Datos de Tiempo Real
  - Interfaz de Operador
  - Comunicaciones con equipos de campo

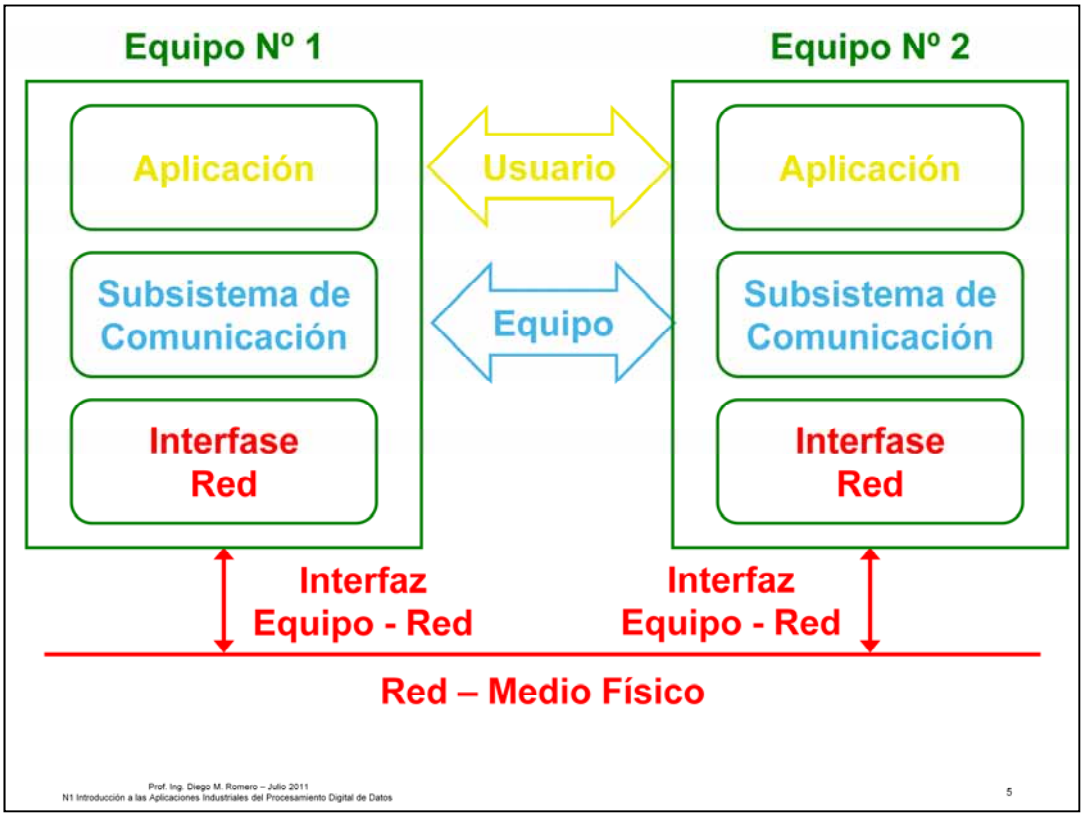
Programa

- Día 4
  - Servidores de datos y registros Entrada/Salida
  - Servidores de datos remotos
  - Programación de Scripts, distintas alternativas
  - Registros de Alarmas y Eventos
  - Registros Históricos
  - Módulos Complementarios
- Día 5
  - Conectividad con bases de datos relacionales
  - Acceso por WEB
  - Criterios para la selección del sistema HMI
  - Demostraciones prácticas

Las redes Ethernet han tenido éxito y son universalmente aceptadas en empresas, universidades y aún en hogares. Pero también es posible encontrarlas en ámbitos industriales. Y su utilidad se basa en la posibilidad de supervisar la calidad de los enlaces, la existencia de utilitarios (p.e. Telnet) para la configuración de los equipos y la capacidad de controlar y programar a los dispositivos desde una ubicación central. Y este tipo de aplicaciones se asociaba hasta no hace mucho con los niveles administrativos, pero cada vez más se lo aplica en piso de planta y a nivel de dispositivos de automatización y control. Como complemento indispensable el “stack” TCP/IP permite la transmisión de las señales de control, la conexión con aplicaciones HMI/SCADA y servidores WEB embebidos en los dispositivos de campo.

Esta fue la evolución de las redes industriales:

1. Redes industriales propietarias.
2. Integración de la información de piso de planta (HMI/SCADA) con los sistemas de gestión (MRP/ERP).
3. Utilización para redes de nivel 1 y 2.
4. Ampliación de la conectividad por medio de servicios WEB e Internet.



¿Qué es una red de datos?

Las redes de datos son un conjunto de computadoras u otros dispositivos digitales de procesamiento de datos que tienen la habilidad de comunicarse entre ellas sobre un medio común.

¿Por qué usar una red de datos?

Las redes permiten COMPARTIR recursos tales como :

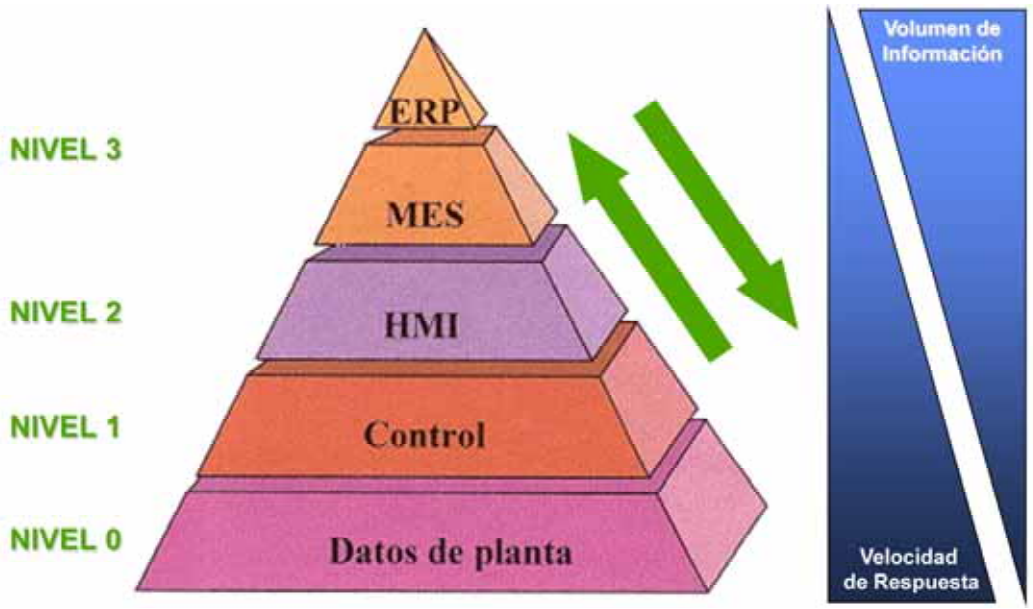
- Dispositivos (Impresoras, módems, almacenamiento, etc.)
- Transferencia de archivos entre sistemas
- Aplicaciones y servicios

Compartir dispositivos implica que se necesita comprar menos hardware.

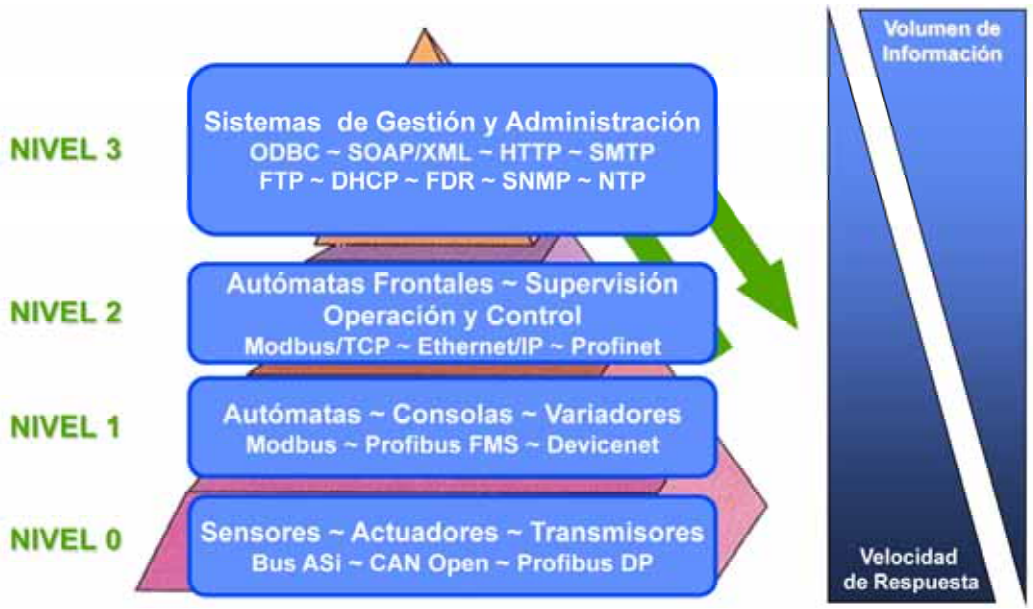
Los elementos de una red de datos

- Dos o más entidades que tengan algo que compartir, por medio de un servicio de red
- Un camino para la comunicación y reglas que permitan el intercambio de la información a compartir, expresadas en un protocolo:
  - El medio físico de conexión (interfase eléctrica, velocidades de transmisión, etc.)
  - La interfase lógica de conexión (direccionamiento, mecanismos de acceso al medio físico, etc.)
  - Los mecanismos normales de intercambio de información
  - Los mecanismos de detección de errores, su corrección y/o retransmisión
  - Pueden aparecer combinados en las llamadas pilas (stacks) de protocolos (por ejemplo el protocolo Modbus/TCP que se monta sobre una red Ethernet y utiliza los protocolos TCP/IP)

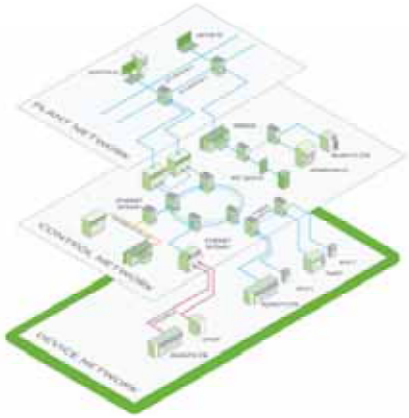
Redes Industriales - Niveles de comunicación

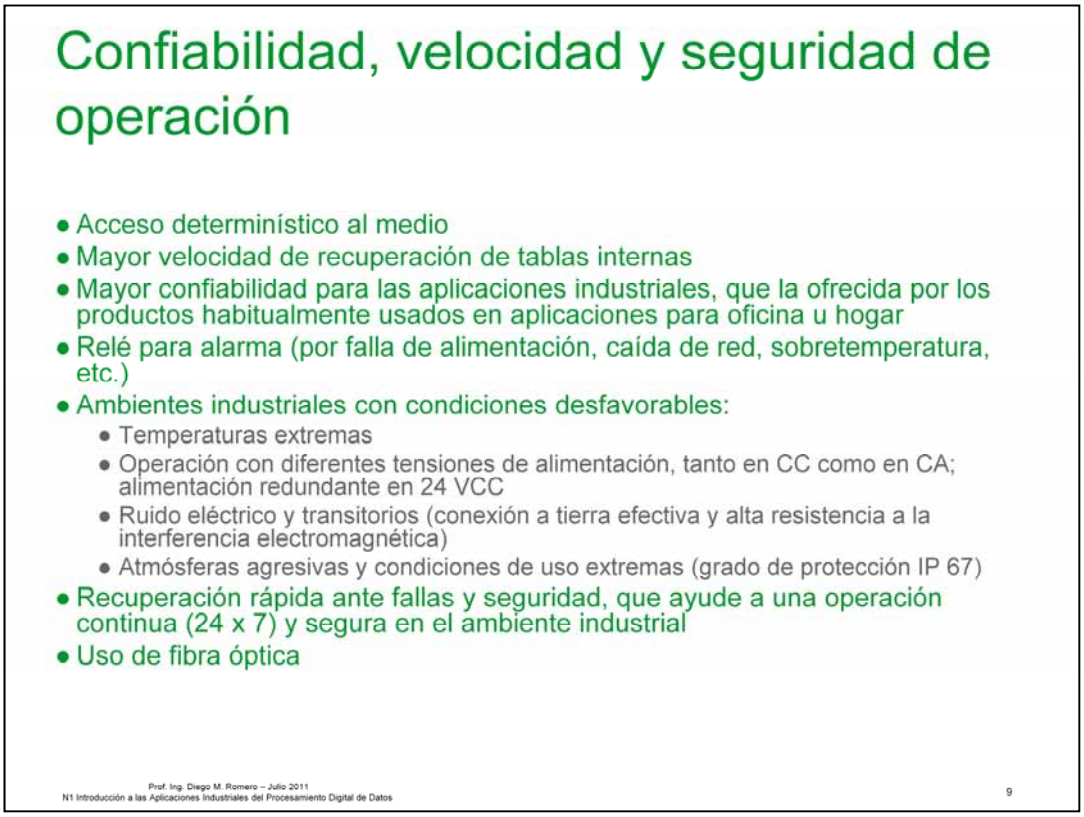


Redes Industriales - Niveles de comunicación



Requerimientos de las redes Ethernet en aplicaciones industriales





Al usar redes Ethernet en aplicaciones de piso de planta, deben distinguirse los requerimientos cuando se las compara las prestaciones del equipamiento comercial disponible, como el usado para la conexión de PCs, printer servers, etc.

Los mismos son diseñados para operar en condiciones ambientales controladas. Si se utiliza ese equipamiento comercial diseñado para aplicaciones de oficina en las condiciones extremas típicas del ambiente industrial, se corre el riesgo de producir fallas serias en el sistema de automatización y control.

Dado que cada dispositivo industrial interconectado (PLCs, variadores de velocidad, arranques inteligentes, etc.) cumple un rol importante en el sistema, la comunicación entre éstos cumple un rol fundamental que no debe descuidarse. Muy diferente a la aplicación típica de oficina, donde una falla de la red, por lo general implica tan sólo que algunas estaciones de trabajo de no puedan enviar correo electrónico por unos minutos. En una aplicación industrial, cuando uno dispositivo conectado en red sufre una falla que lo aísla del resto, aún por brevísimos períodos de tiempo, pueden producirse grandes perjuicios económicos y afectarse la integridad de personas e instalaciones.

Conectividad y facilidad de uso

- Fácil Instalación y Mantenimiento:
  - Mayor granularidad de puertos
  - Montaje en racks, riel DIN y gabinetes industriales
  - Reportes dinámicos de estado que informen sobre el funcionamiento de equipos y dispositivos, que eviten fallas del sistema y pérdidas de información
  - Funciones de administración incorporadas para facilitar el manejo de las redes Ethernet industriales
  - Administración simple e integrada con sistemas existentes
- Diagnóstico simple para personal no entrenado en TI
- Automatización de diagnósticos específicos y recuperación rápida de fallas por el personal de mantenimiento
- Costos de entrenamiento reducidos
- Reemplazo rápido de dispositivos, con reconfiguración automática (FDR)
- Soporte de protocolos de "Capa de Aplicación"
- Conexión de equipos existentes sin conectividad a Ethernet

Aspectos a considerar

Redes Industriales vs. Comerciales

- Estándares y ensayos
- Arquitecturas y condiciones de operación
- Características del tráfico de datos
- Configuración de dispositivos
- Localización y diagnóstico de fallas

Algunas especificaciones comparadas

	Comercial / Oficina	Industrial
Ensayos Vibración y Choque	**N/D**	**SI**
MTBF	**5 años**	**> 20 años**
Vida útil esperada	**5 años**	**> 10 años**
Compatibilidad Electromagnética (EMC)	**EN 55024**	**IEC 1000-4-2 IEC 1000-4-6 IEC 1000-4-4 EN 61000**
Certificaciones UL	**UL 60950 (IT)**	**UL 508 (Industrial)**
Áreas peligrosas	**N/A**	**UL 1604 Clase 1 División 2**
Certificación Uso Marino (GL)	**NO**	**SI**
IEC 61133-2 (ensayos para uso industrial)	**NO**	**SI**
Aplicaciones para subestaciones (EMC según IEC61850)	**NO**	**SI**

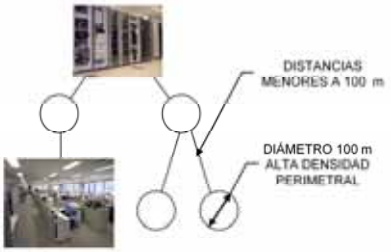
Comparando Arquitecturas

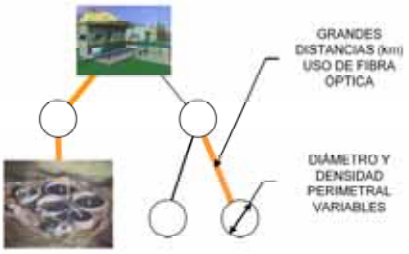
- Comercial

Puertos perimetrales	**MUCHOS**
Tipo de cable	**UTP**
Recuperación	**1 - 60 s**
Temperatura Operación	**0 - 45 °C**
Humedad / Polvo	**NO**
Montaje	**Rack 19"**
Alimentación	**220 VCA**
Alimentación Redundante	**Opcional**
Puesta a tierra	**NO**
EMC	**BAJA**

- Industrial

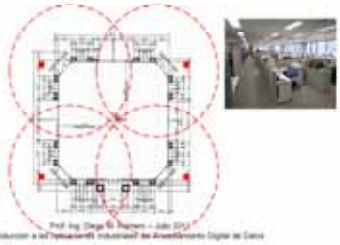
Puertos perimetrales	**POCOS**
Tipo de cable	**STP y F. O.**
Recuperación	**< 500 ms**
Temperatura Operación	**0 - 60 °C**
Humedad / Polvo	**SI**
Montaje	**Riel DIN**
Alimentación	**12 - 30 VCC**
Alimentación Redundante	Estándar
Puesta a tierra	**SI**
EMC	**ALTA**



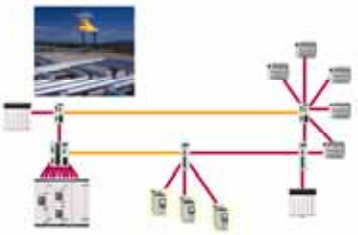


Comparando Arquitecturas

- Comercial
  - Switches de alta densidad con puertos sin usar
  - Cableado UTP estándar limitado a 100 m no siempre apto para uso industrial
  - Caminos redundantes por STP o RSTP, lentos para control industrial
  - Los ventiladores acumulan polvo
  - Sin opción IP 67
  - Sin montaje en riel DIN
  - Alimentación sólo en CA, no redundante en switches perimetrales
  - Tierra separada
  - Baja tolerancia a la interferencia electromagnética



- Industrial
  - Switch con densidad acorde con las aplicaciones
  - Grandes distancias con el uso de fibra óptica mono y multi modo
  - Camino en anillo redundante de recuperación rápida (< 0,5 s)
  - Rango de temperatura extendida
  - Grado de protección IP 67 contra polvo y humedad
  - Montaje en riel DIN
  - Alimentación en baja tensión (24 VCC), redundante
  - Conexión de tierra y STP
  - Alta tolerancia a la interferencia electromagnética

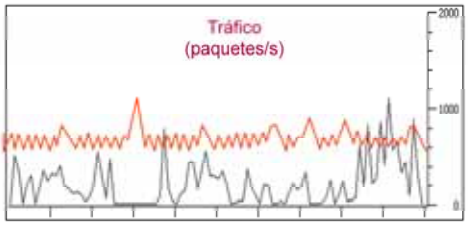


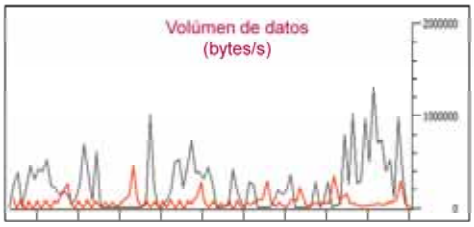
STP: Spanning Tree Protocol (recuperación no menor a 30 s)

RSTP: Rapid Spanning Tree Protocol (recuperación no menor a 1 s)

Volúmen de Datos y Tráfico

- Comercial
  - Prioridad de tráfico para VoIP y bases de datos
  - La red y los servidores deben permitir la transferencia de grandes archivos, con baja ocurrencia
- Industrial
  - Protección contra Broadcast y filtrado de Multicast
  - Tráfico prioritario de la comunicación entre dispositivos perimetrales
  - Bajo volúmen de datos, con alta ocurrencia

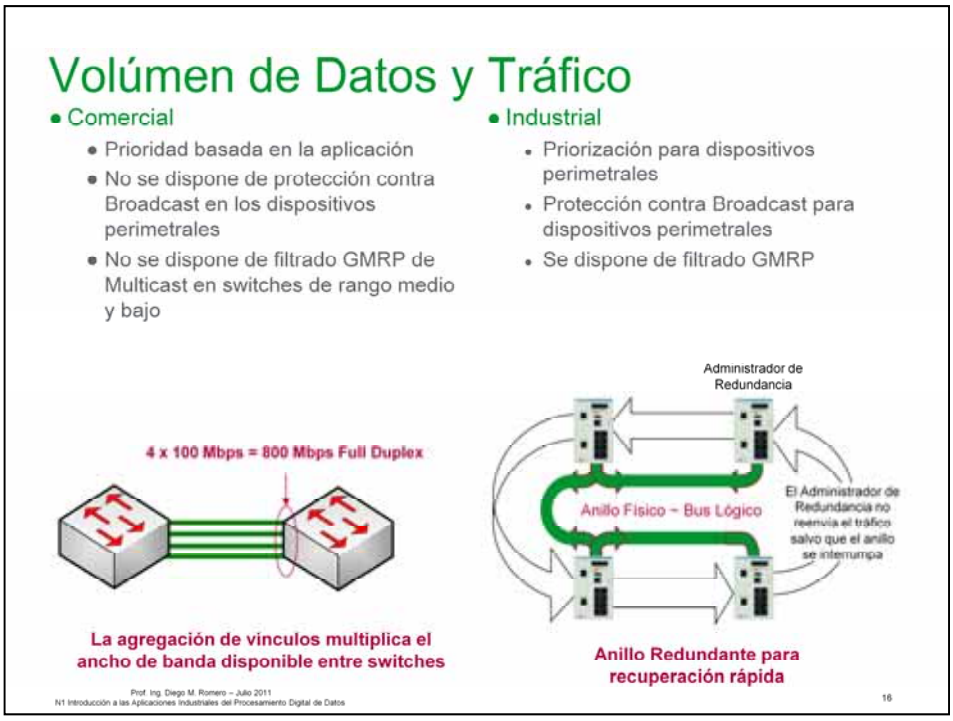




DISPOSITIVO PERIMETRAL COMERCIAL

DISPOSITIVO PERIMETRAL INDUSTRIAL

VoIP: Voz sobre IP o Voice on IP



GMRP: GARP Multicast Registration Protocol

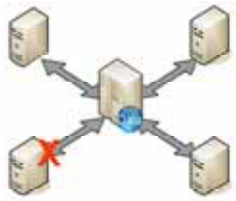
- Protocolo de control de tráfico multicast a nivel 2 equivalente a IGMP Snooping y CGMP; definido por el IEEE 802.1
- Realiza el registro y el borrado de los grupos multicast en el nivel 2
- Configurado en el ordenador y en el switch
- Se generan peticiones de nivel 2 equivalentes a las generadas a nivel 3 por IGMP
- El switch recibe ambas y registra los puertos involucrados

GARP / GVRP: Group Address Registration Protocol

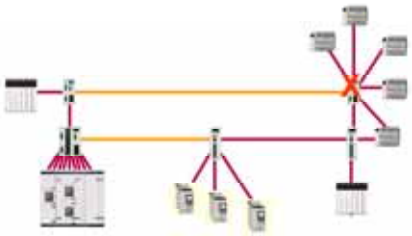
- Conocido como **Protocolo de Registro VLAN** o **Protocolo Genérico de Registro de VLAN** es un protocolo que facilita el control de redes locales virtuales (VLANs) dentro de una red grande
- Incluído en la norma IEEE 802.1Q, la cual define el método para marcar las tramas dentro de los datos de configuración de la VLAN
- Permite que los switches intercambien información de configuración de la VLAN dinámicamente con los demás equipos que conforman la red

Localización y reparación de fallas

- Comercial
  - Los dispositivos perimetrales no son tratados como críticos
  - La reparación puede tomar hasta 48 horas
  - El diagnóstico requiere de personal especializado en IT y equipamiento específico
- Industrial
  - Todos los dispositivos son tratados como críticos
  - La reparación no debe llevar mas que 1 a 4 horas
  - El diagnóstico y la reparación la realiza personal de mantenimiento de planta poco entrenado en IT



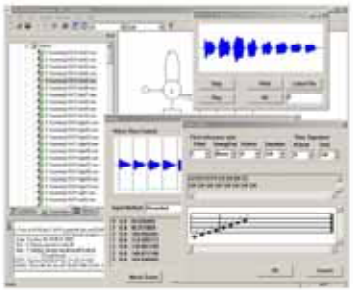
Falla de un dispositivo perimetral en una red comercial



Falla de un dispositivo perimetral en una red industrial

Localización y reparación de fallas

- Comercial
  - Herramientas de supervisión complejas
  - Sólo se supervisan los dispositivos centrales
  - **BAJA** prioridad para los dispositivos perimetrales
  - Mesa de Ayuda de IT no familiarizado con equipamiento industrial
- Industrial
  - Herramientas de supervisón y diagnóstico simples
  - Supervisión de todos los dispositivos
  - **ALTA** prioridad para todos los dispositivos
  - El personal de mantenimiento de planta localiza las fallas en los switches y dispositivos perimetrales



Reemplazo del equipamiento

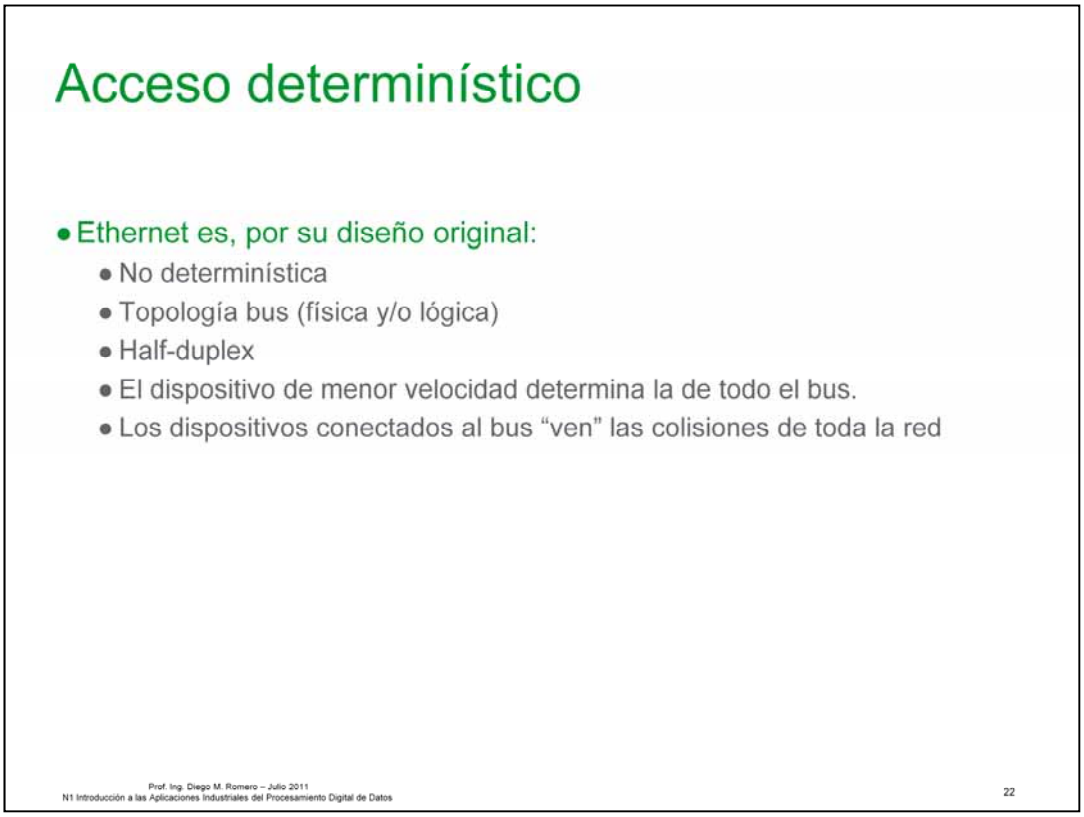
- Comercial
  - Requiere el manejo de herramientas complejas
  - Debe tenerse un **ALTO** conocimiento de redes informáticas
  - Recursos humanos entrenados
  - Hasta 48 horas para resolver las fallas en dispositivos perimetrales
- Industrial
  - Saber usar un navegador WEB
  - Alcanza con un conocimiento **BAJO** de redes informáticas
  - A cargo personal de mantenimiento de planta
  - No más de 4 horas las fallas en dispositivos perimetrales

Reemplazo del equipamiento

- Comercial
  - **ALTA** complejidad en el reemplazo de switches y de dispositivos perimetrales
  - La Mesa de Ayuda ingresa en una lista de espera los problemas reportados
  - Consola de configuración de uso complejo, que requiere personal entrenado
- Industrial
  - **BAJA** complejidad en el reemplazo de switches y de dispositivos perimetrales
  - el personal de mantenimiento de planta puede reemplazar rápidamente los switches y los dispositivos perimetrales
  - Interfaz gráfica con ayuda en línea para la configuración

```
R1(config)#ip routing
  // 2. configure subinterface
R1(config)#int fa0/0.1
R1(config-subif)#encapsulation
dot1q 1
R1(config-subif)#ip add
192.168.0.1 255.255.255.0
R1(config-subif)#no shut
R1(config-subif)#exit
```

Características de los Switches Ethernet Industriales



Ethernet utiliza un medio físico único, compartido entre todos los dispositivos que desean intercambiar información, y para lo cual todos tienen igual prioridad. Por lo tanto debe existir algún mecanismo para evitar conflictos en el envío de los paquetes de datos y proteger la integridad de los datos. Cada nodo determina cuando la red está disponible para el envío de paquetes. Siempre existe la posibilidad que dos o más nodos intenten transmitir al mismo tiempo, lo que resulta en una colisión.

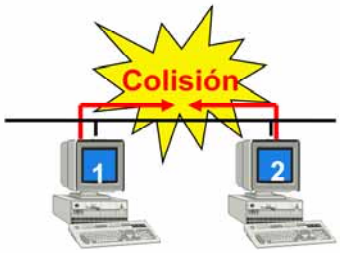
Reducir al mínimo (e idealmente eliminar) las colisiones es un factor crucial en el diseño y la operación de las redes de datos. Un aumento de la colisiones es a menudo consecuencia de una gran cantidad de nodos en la red, compitiendo entre si por el ancho de banda disponible. Esta situación reduce la prestación general de la red, haciendo que cada nodo la perciba como más lenta. La segmentación de la red, dividiéndola en sectores unidos entre si por medio de un bridge o switch, es una de la formas de mejorar esta situación desfavorable.

Durante mucho tiempo Ethernet no se consideró una alternativa válida para aplicaciones industriales pues fue concebida para aplicaciones de oficina. Esto es, su diseño sólo la hacía apta para entornos donde las PCs y otro equipamiento de oficina operaran sin problemas, una oficina, el hogar o centros de cómputos climatizados. La regla era entonces “el equipamiento Ethernet comercial no es apto para las más demandantes aplicaciones industriales”.

Acceso determinístico

¿Qué es CSMA/CD?

- CSMA/CD - Acceso Múltiple por Detección de Portadora con Detección de Colisiones, (Carrier Sense Multiple Access with Collision Detection)
- Es un método de control de acceso al medio físico (red) no determinístico
- Un dispositivo que quiere transmitir un mensaje "escucha" la red para detectar si algún otro equipo está transmitiendo:
  - Si la red está limpia, el dispositivo inicia la transmisión
  - El dispositivo "escucha" su propio mensaje para saber si ocurrió una colisión
  - Si no se detecta una colisión, se realiza el proceso; Si se detecta la colisión, entonces el dispositivo espera un tiempo aleatorio y reintenta



Prof. Ing. Diego M. Romero – Julio 2011
N1 Introducción a las Aplicaciones Industriales del Procesamiento Digital de Datos

23

En su especificación original, Ethernet era half-duplex y estaba concebida para una topología de tipo bus compartido. Esto obligó a incluir un mecanismo para administrar el acceso a ese medio físico compartido permitiendo "detectar y eliminar las colisiones". El mecanismo elegido fue **CSMA/CD**, Acceso Múltiple por Detección de Portadora con Detección de Colisiones (**C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection).

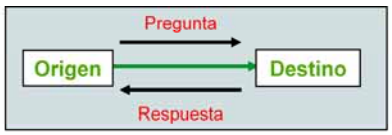
Este mecanismo de control de acceso al medio físico es muy diferente al simple y conocido de las interfases serie RS-232/RS.422/RS-485, muy usado durante años en equipos de automatización y control. Y justamente por esta razón, Ethernet fue resistida durante mucho tiempo por los automatistas, favoreciendo interfaces propietarias y cerradas.

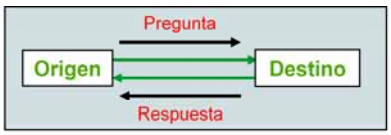
La tecnología actual de Ethernet, sin embargo, es full-duplex, existe en topología estrella, y aún con CSMA/CD, opera a mayores velocidades de transmisión, de 100 Mbps y 1 Gbps (con 10 Gbps en desarrollo). Y como se verá más adelante en esta presentación, el uso de switches Ethernet de alta prestación, permite asilar a los diferentes dispositivos conectados a la red permite obtener un comportamiento cuasi-determinístico.

Estas nuevas características de Ethernet, sumadas a que la misma es una tecnología probada, aceptada universalmente para la interconexión de equipos digitales e intercambio de datos, han permitido una creciente penetración en ámbitos de automatización y control.

Half-Duplex vs. Full-Duplex

- **Half-Duplex:**
  - La información puede transmitirse en ambos sentidos, pero no simultáneamente
  - Una transmisión half-duplex usa el mismo canal (físico o lógico) para la comunicación
  - Un walkie-talkie es un dispositivo half-duplex ya que puede hablar solamente una persona a la vez
- **Full-Duplex:**
  - La información puede transmitirse en ambos sentidos, simultáneamente
  - Una transmisión full-duplex utiliza diferentes canales (físicos o lógicos) para la comunicación
  - El teléfono es un ejemplo de dispositivo full-duplex





Prof. Ing. Diego M. Romero – Julio 2011
N1 Introducción a las Aplicaciones Industriales del Procesamiento Digital de Datos

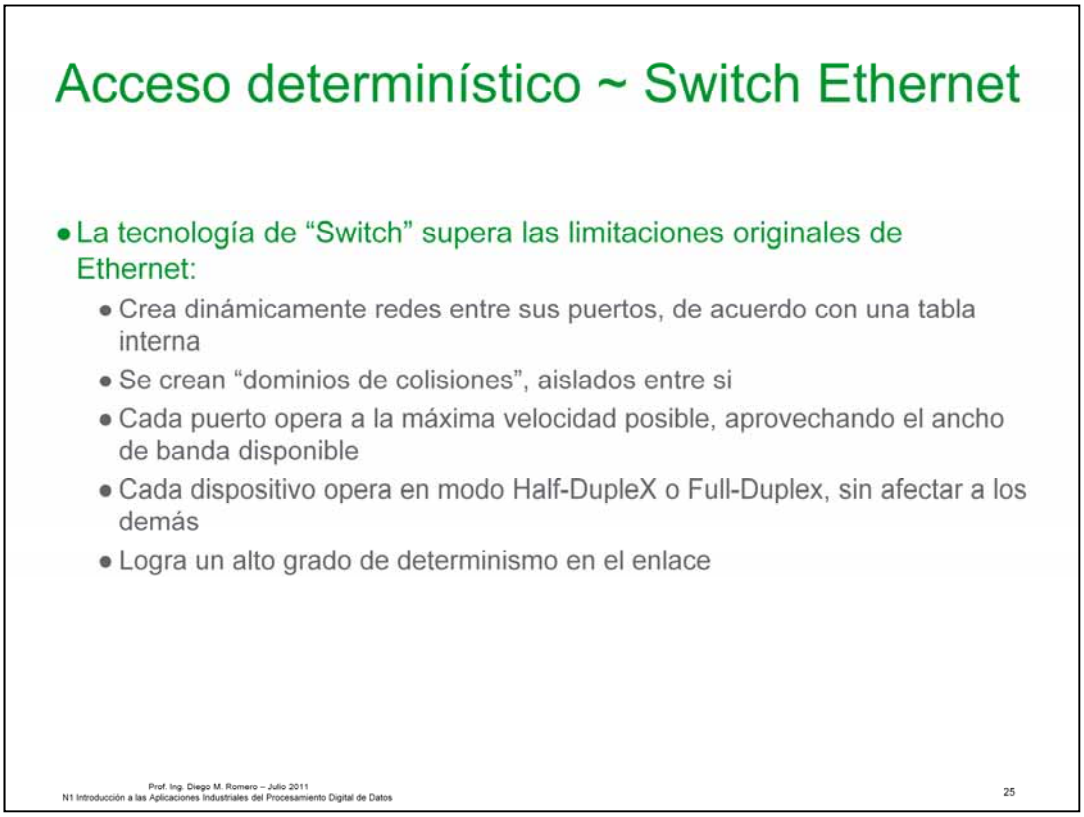
24

Half-Duplex

El protocolo Modbus serie (ASCII ó RTU) es un ejemplo de una comunicación **half-duplex**. El Maestro Modbus debe esperar que el Esclavo direccionado responda, antes de enviarle un nuevo comando.

Full-Duplex

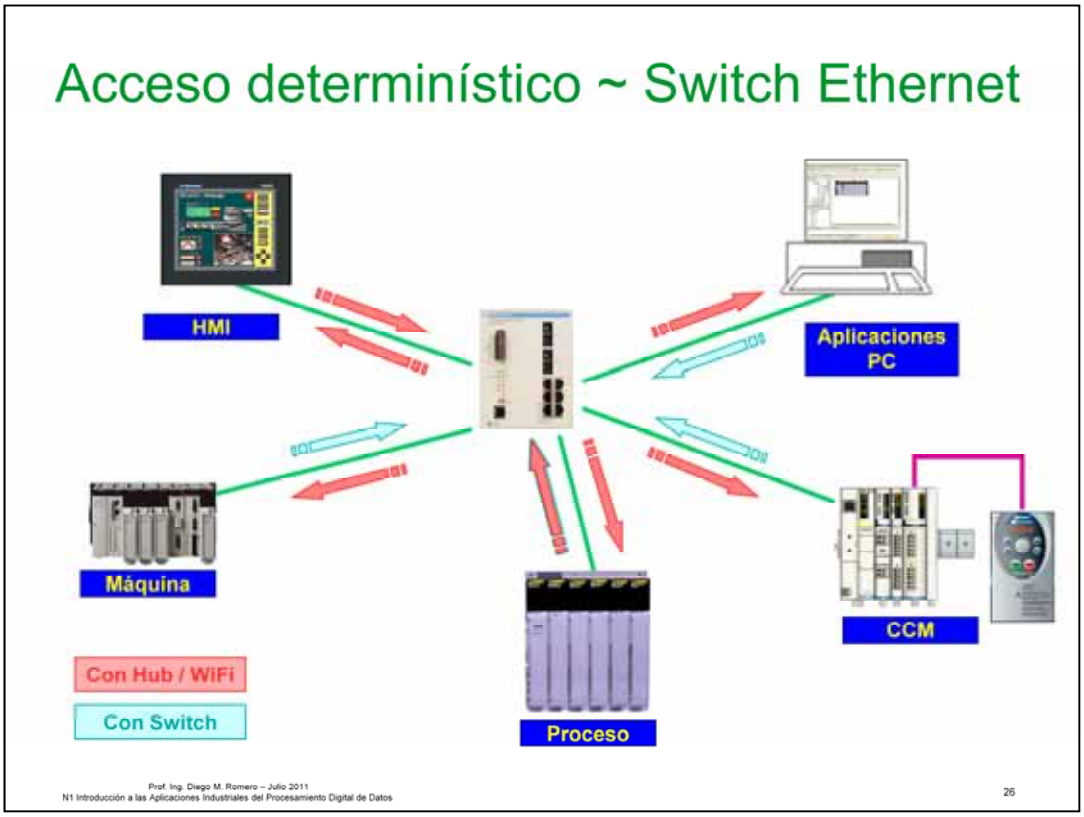
Su utilización sobre un único canal físico, exige la utilización de algún mecanismo para la separación de las señales recibida y transmitida. Por esta razón, o cuando se utilizan dos canales físicos, la comunicación full-duplex siempre requiere utilizar hardware adicional.



Hay diferentes formas de mejorar el problema del acceso determinístlco al medio, creado por la técnica CSMA/CD. En primer lugar debe considerarse la forma en la que los datos son transmitidos entre los diferentes dispositivos de la red. Ethernet fue concebida originalmente como half-duplex, por lo cual un dispositivo NO PUEDE transmitir y recibir datos simultáneamente. Pero hoy Ethernet es **full-duplex**, permitiendo que cualquier dispositivo inicie el envío de una nueva trama de datos mientras continúa con la recepción o viceversa. Este comportamiento permite decir que un dispositivo Ethernet operando en full-duplex a 100 Mbps, dispone en realidad de un ancho de banda teórico de 200 Mbps, ya que puede recibir y transmitir simultáneamente a 100 Mbps.

Otra forma es reducir la probabilidad de una colisión, es disminuir el número de nodos conectados al mismo segmento de red. Al disminuir el número de nodos, la probabilidad de que dos nodos inicien una transmisión simultáneamente disminuye. Y si se pudiera conectar un único nodo de red a cada segmento, las colisiones se eliminan.

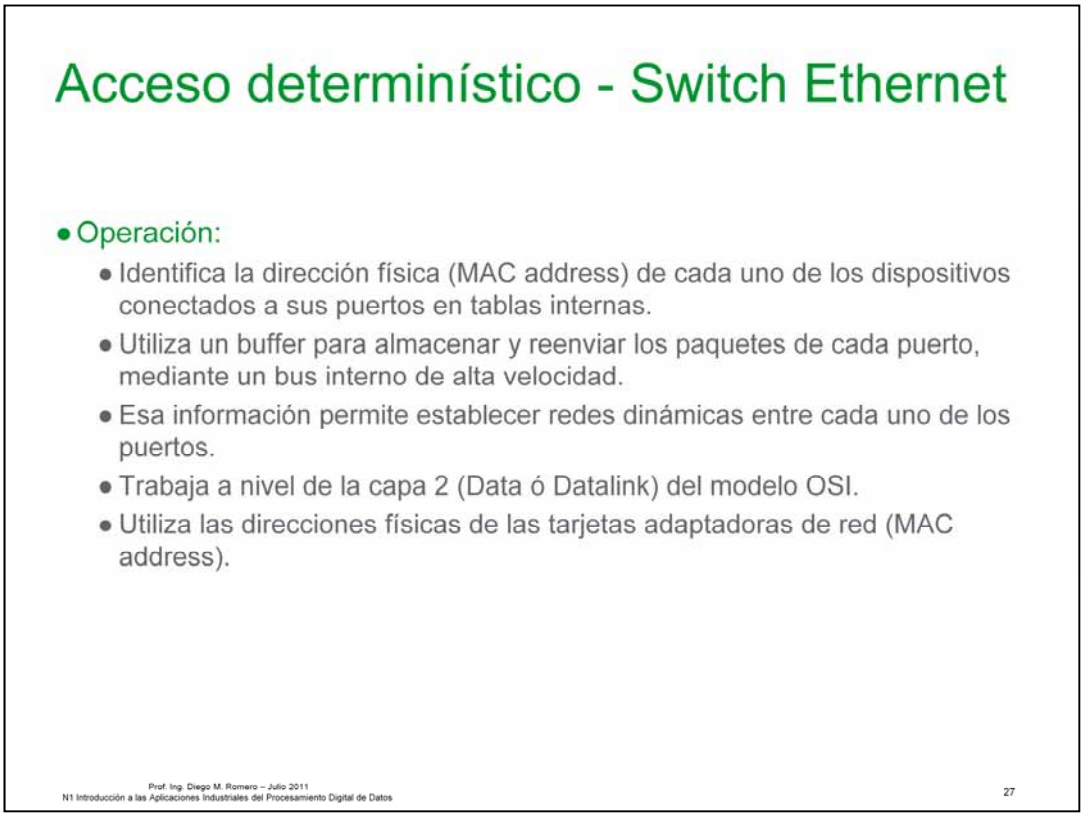
¿Cómo lograr que haya un único nodo por segmento de red? Utilizando un **switch Ethernet**, para aislar a un número reducido de nodos (idealmente un único nodo) en lo que se llama “dominio de colisión”. Un switch es un equipo especializado que tiene múltiples puertos Ethernet, un procesador dedicado, un bus interno de muy alta velocidad y una memoria rápida de lectura/escritura. Inicialmente cada una de las tramas recibidas por el switch es reenviada a todos los puertos del switch, pero al recibir la repuesta a las mismas, “aprende” por cual de sus puertos recibió la correspondiente a cada **dirección física (MAC address)** asociándolas. A partir de ese momento, el switch reenviara las tramas considerando la dirección física de destino para decidir por cual de sus puertos (y sólo por ese) las reenviará. Estas características lo diferencian de un hub el cual, también con un cierto número de puertos, actúa tan sólo como un repetidor eléctrico, reenviando SIEMPRE a todas sus puertos las tramas recibidas por uno de éstos.



A modo de ejemplo se compara el funcionamiento de un Hub (o una conexión Ethernet inalámbrica) con un switch. Las condiciones son:

1. Desde la PC se programa y se pone a punto la aplicación del PLC que controla una máquina compleja.
2. Desde el PLC que comanda el proceso se accede por medio de Ethernet a los dispositivos de un CCM inteligente que forma parte del automatismo.
3. El panel de operación gráfico lee y escribe variables del PLC que comanda el proceso.

Ver animación completa en archivo **IntroEthIndSwitch.avi** adjunto.



Ethernet puede ser visto como un “igualador”, ya que todos los dispositivos interconectados (incluyendo las PCs, servidores, PLCs, sensores, actuadores, terminales de diálogo, etc.) en la misma red local (LAN) Ethernet se encuentran en igualdad de condiciones para enviar y recibir información. Esto es así porque hay una cantidad máxima de datos que pueden enviarse en una red Ethernet en cada transmisión y por otro lado el primero que toma control de la red es el primero en utilizarla. La conexión de las PCs ubicadas en el piso de planta y otros dispositivos a la red corporativa, les permite a los ingenieros acceder a Internet, herramientas d gestión y mantener un fluído contacto por medio del correo electrónico. Brinda además la posibilidad a otras áreas de acceder a la información de piso planta relevante para sus tareas.

¡Pero atención...! Esta arquitectura totalmente abierta puede impactar negativamente en el intercambio de datos critico entre los dispositivos de automatización y control. El tráfico corporativo de correos electrónicos, accesos a bases de datos, mensajería instantánea, accesos WEB, movimiento de archivos, etc. tiene características y requerimientos muy diferentes al generado en le piso de planta.

A continuación se presentarán esos requerimientos y se dará las características de los switches Ethernet para aplicaciones industriales.

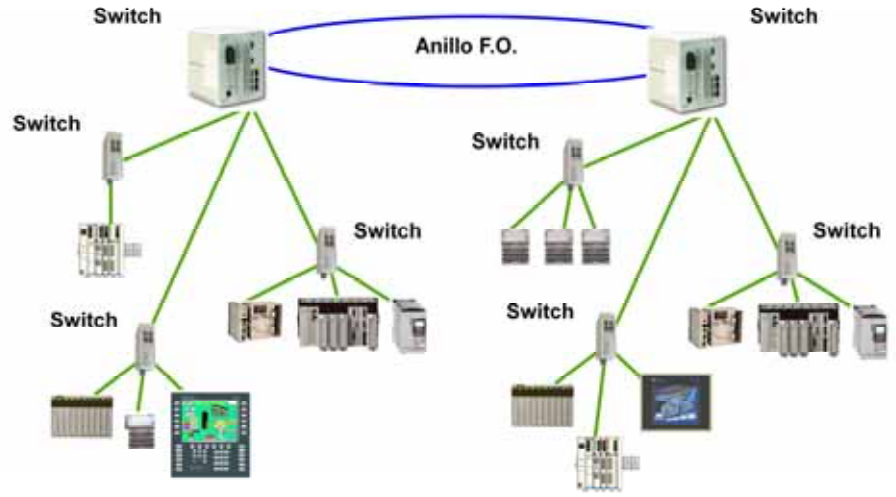
Un Switch Ethernet Industrial puede ser usado para aislar efectivamente aquellos dispositivos claves del sistema de automatización en su propio dominio de colisiones, trabajando en modo full-duplex a su máxima velocidad posible. Los ingenieros de proyecto y de mantenimiento pueden acceder de todos modos a esos dispositivos.

En este tipo de aplicación cada dispositivo es conectado a un puerto exclusivo del switch Ethernet, aislándolo del resto del tráfico de la red Ethernet. Así es como un switch Ethernet multipuerto permite la conexión del PLC con sus sensores/actuadores. Salvo por esporádicos accesos para configuración y/o reprogramación recibidos desde otros nodos, el switch mantiene al PLC y sus elementos asociados totalmente aislados del resto de la red.

Todos los switches Ethernet poseen puertos que pueden operar a 10 Mbps ó 100 Mbps, permitiendo la interconexión de dispositivos que operan a diferentes velocidades, sin afectar a los más rápidos. Lo mismo ocurre con aquellos dispositivos que sólo operan en modo half-duplex. Y los puertos de cobre o fibra que operan a 1 Gbps permiten la interconexión entre si de switches que vinculan entre si dos áreas o sectores separados físicamente. Este enlace de 1 Gbps, operando en modo full-duplex, permite el intercambio de datos entre switches, de hasta diez conexiones simultáneas a 100 Mbps cada una, sin colisiones.

El uso de puertos de fibra óptica brinda como ventaja principal la inmunidad absoluta al ruido eléctrico y la eliminación de lazos de masa. Permiten superan además el límite de 100 metros de los puertos Ethernet de cobre, extendiendo los enlaces a varios cientos de metros e incluso a varios kilómetros.

¿Dónde usar un switch industrial?



Priorización de mensaje según IEEE 802.1p

Permite dar prioridad a los datos provenientes de determinado dispositivo con respecto a otros conectados a la red, acelerando la transferencia. Con esta funcionalidad se impide que las tramas de alta prioridad se vean interrumpidas por el tráfico de los de menor prioridad. El switch puede procesar y enviar todos los paquetes de mayor prioridad antes de hacerlo con los de menor prioridad o alternar entre unos u otros.

Priorización de puerto

Le asigna una prioridad a cada mensaje, basada en el puerto de origen, sin tener en cuenta la asignada por los dispositivos conectados a éste. Permite asignar prioridades a dispositivos que no soportan la norma IEEE 802.1p. Se requiere configurar el switch para esta función. Los paquetes sin información de prioridad (VLAN o marca de prioridad) se transmiten según la prioridad asignada a cada puerto. Es posible asignarle una prioridad diferente a cada puerto.

VLANs:

Las redes virtuales (VLANs) está basadas en establecer vínculos lógicos (en vez de físicos) y constituyen elementos flexibles en el diseño de las redes. La mayor ventaja de las VLANs es la posibilidad de crear grupos de usuarios de acuerdo con un criterio funcional y no por su ubicación física o forma de acceso a la red. Las mismas están definidas en el estándar IEEE 802.1Q. Incluye el filtrado de las tramas de tráfico broadcast y multicast, limitándolos a los nodos que integran la VLAN. El mismo dispositivo puede ser integrante de más de una VLAN:

Refresco rápido de las tablas de enrutameinto

Al perderse el vínculo con un dispositivo conectado a un puerto, todas las direcciones respectivas almacenadas en la tabla de enrutamiento son eliminadas. Los beneficios son:

- Esta funcionalidad resulta de gran utilidad cuando se eliminan o cambian de ubicación dispositivos conectados al switch
- La estación que se cambió de puerto es alcanzada de inmediato
- No hay interrupciones (timeout)
- Asiste en la ejecución del algoritmo ”Spanning Tree” y anillos redundantes.

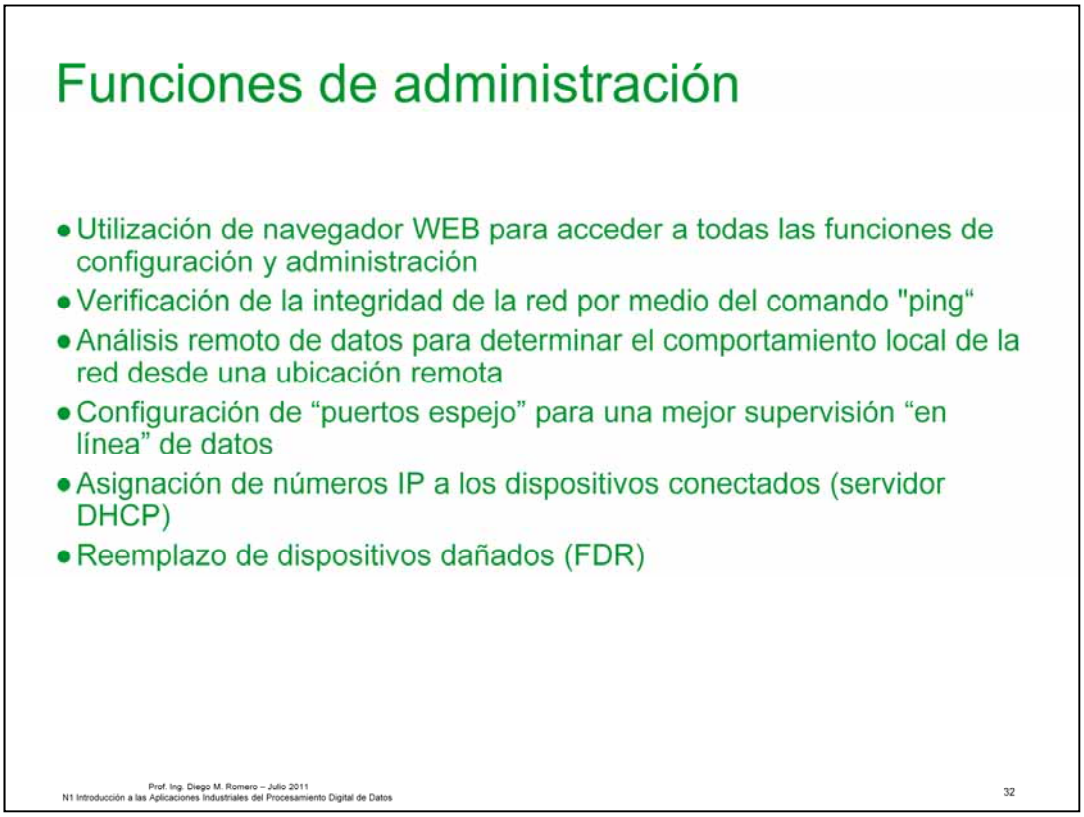
Recuperación rápida de fallas funcionales

Sólo mencionan los puntos principales de mayor confiabilidad para aplicaciones industriales. Al considerar las comunicaciones en el ámbito industrial, mayor confiabilidad no sólo significa un gabinete más robusto y tolerancia a temperaturas extremas, sino que involucra además una mayor tolerancia a fallas funcionales. En una oficina, una falla de comunicación que dure 3 minutos es apenas un inconveniente menor, en tanto que en una aplicación industrial esos mismos 3 minutos podrían ser catastróficos. Teniendo esto en cuenta, las funciones de auto recuperación resultan esenciales para mantener la red en funcionamiento.

Reportes dinámicos

Dado que los dispositivos Ethernet conectados a un red Ethernet industrial pueden estar ubicados en puntos extremos de ésta, no siempre es posible conocer su estado de funcionamiento en lo que hace a la comunicación. Esto significa que el equipamiento Ethernet que conecta a los mismos debe tomar la responsabilidad de proveer a los encargados del mantenimiento con mensajes de alarma en tiempo real. Aún cuando los automatistas se encuentren alejados de la Sala de Control por períodos prolongados de tiempo, ellos deben ser informados del estado de los dispositivos casi instantáneamente en caso que ocurran excepciones.

La forma convencional de determinar ele stado de los diferentes dispositivos es interrogarlos periódicamente, pero esto no es eficiente ni garantiza un reporte de excepciones en tiempo real. Debe poderse generar mensajes de advertencia disparados por tales eventos de excepción.



Ping

La búsqueda de fallas en una red que experimenta problemas puede ser muy compleja para el personal de mantenimiento, sobretodo si no está entrenada en tecnología informática. La rápida solución de estas fallas es particularmente importante en aplicaciones industriales, ya que al interrumpirse la comunicación, pueden detenerse las líneas de producción o comprometerse la seguridad de personas e instalaciones. El primer inconveniente con el que se encuentra el personal de mantenimiento es encontrar rápidamente y de forma confiable cual es el segmento de la red con fallas. El comando "ping" generado desde los dispositivos claves de la red provee una herramienta esencial de diagnóstico.

Análisis remoto de datos

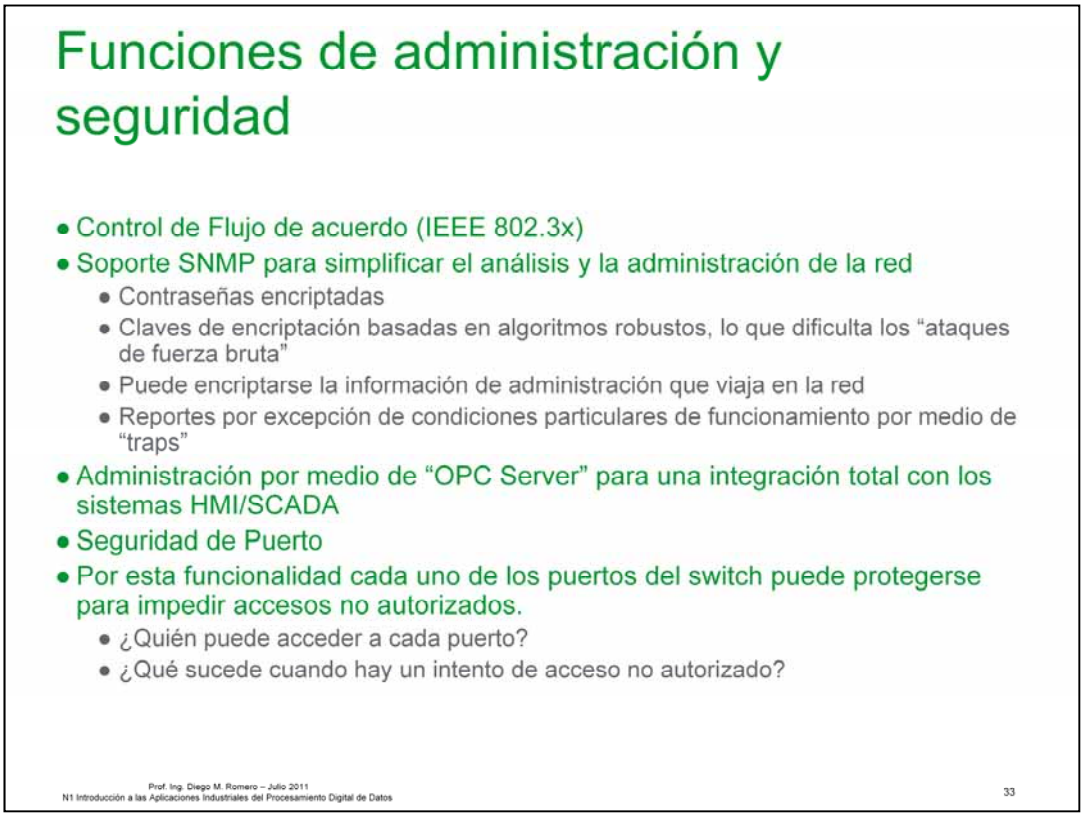
La supervisión remota de los dispositivos de red y sus respectivos enlaces es otra herramienta útil en caso de fallas. Esta herramienta puede residir tanto en una PC (como por ejemplo el software de distribución libre Ethereal) como en los dispositivos claves de la red. Las mismas permiten iniciar la captura de tramas en el red con determinadas condiciones de disparo, registrar las mismas con marca de tiempo, filtrar según las condiciones más convenientes en cada caso. Las herramientas de captura que corren en PC (Sniffers) permiten realizar además un análisis de cada trama a nivel de cada uno de los protocolos involucrados.

Puertos Espejo

En muchas situaciones, sobretodo en la puesta en marcha de una nueva aplicación, es necesario analizar el tráfico entre dos o más dispositivos. Por las características básicas de los switches, esto no es posible. El espejado permite configurar algunos puertos para que repitan el tráfico de otro, facilitando el uso de las herramientas de captura y análisis.

DHCP y Reemplazo de Dispositivos Dañados (FDR)

La configuración de la dirección IP es otro aspecto que debe ser tenido en cuenta en cualquier red que opere bajo ese protocolo. Pero a diferencia del equipamiento de oficina, los dispositivos industriales que se conectan a una red son “cajas negras” sin una interfaz amigable para esta tarea. La inclusión del servicio DHCP, como servidor, en el switch simplifica esta tarea. Como complemento, es posible no sólo asignar el número IP sino también configurar un dispositivo nuevo cuando se reemplaza uno similar que falló. Esto se realiza asignándole un **“nombre de rol (rol name)”** a cada dispositivo. Ese nombre de rol, por medio de la Opción 82 del servicio DHCP y el protocolo TFTP. Esto facilita notablemente las tareas de mantenimiento por parte de personal no especializado en tecnología informática.



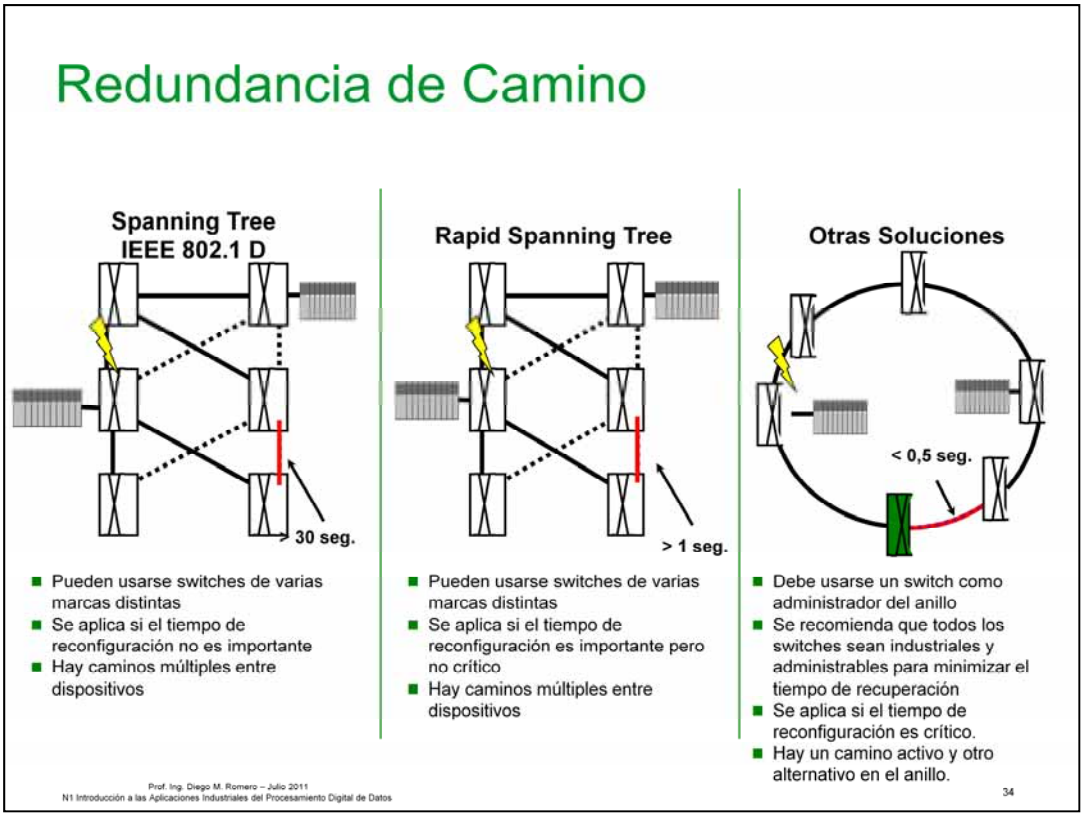
SNMP (Simple Network Management Protocol)

Este protocolo es el más popular entre los profesionales de tecnología informática para la administración remota y análisis de redes complejas. De hecho, incluye una gran variedad de parámetros definidos para esas funciones. Para cada dispositivo administrable por intermedio de este protocolo existe un archivo denominado MIB, con el listado de tales parámetros.

Si bien son muchas las funcionalidades disponibles en un switch administrable, es esta la que define la condición de administrable.

OPC Server

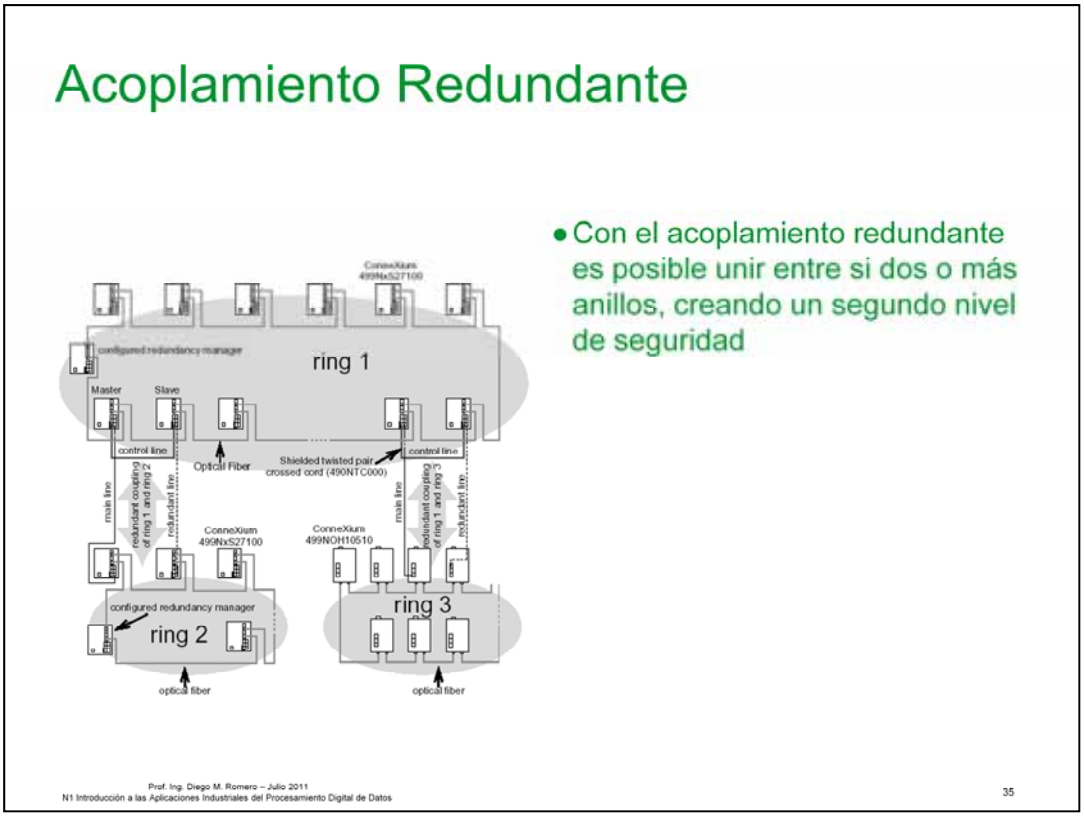
La especificación OPC consiste en un conjunto de estándares abiertos, que cuentan con el soporte de un gran número de fabricantes y usuarios. Es una tecnología de comunicación basada en Microsoft® COM/DCOM y luego en una arquitectura orientada a servicios (SOA en inglés) que utilliza SOAP y HTTP. Es de aplicación en el campo del control y supervisión de procesos; permite que diferentes fuentes de datos sean accedidas, en un esquema Cliente-Servidor, permitiendo el intercambio de datos con un determinado equipo de campo en su protocolo específico. Con el uso de servidor OPC server que permita el acceso al protocolo SNSMP es posible administrar y supervisar diferentes dispositivos de red, desde el software HMI.



Spanning Tree
Es el nombre de un algoritmo empleado en la determinación de los caminos posibles en una red Ethernet compleja. Está especificado en la norma IEEE 802.1 D. Este algoritmo impide la circulación de tramas en la red Ethernet, cuando existen caminos múltiples (redundantes), deshabilitando los puertos que sena necesarios. Así mismo determina el camino óptimo entre todos los posibles. Cuando se produce una falla o interrupción en ese camino, se elige uno alternativo aplicando ese algoritmo. Típicamente esa reconfiguración lleva de 30 a 90 segundos.
El **Spanning-Tree Protocol (STP)** evita la formación de lazos al conectar los switches entre si por caminos múltiples. El algoritmo garantiza que en todo momento haya un único camino activo entre dos dispositivos de red.

El **Rapid Spanning-Tree Protocol (RSTP)** es una variante mejorada del algoritmo que permite un tiempo de recuperación más corto, del orden del segundo.

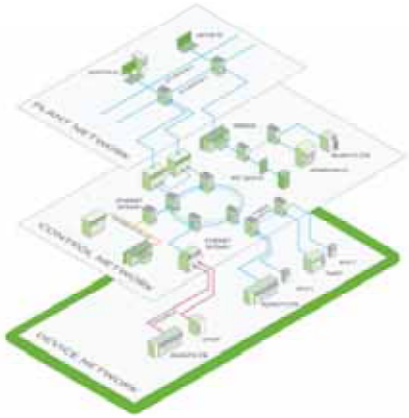
Otras Soluciones
Para mejorar la velocidad de respuesta existen soluciones alternativas, desarrolladas por cada fabricante, basadas en estructuras de anillo. En esta arquitectura cada componente de la red se conecta a un anillo formado por switches. Uno de eso switches es el responsable de administrar el anillo y evitar la circulación de tramas. Los switches restantes pueden ser comunes, inclusive de tipo comercial y/o no administrables. Sin embargo resulta conveniente utilizar switches industriales y administrables por su mayor velocidad de reconfiguración de la tabla interna.



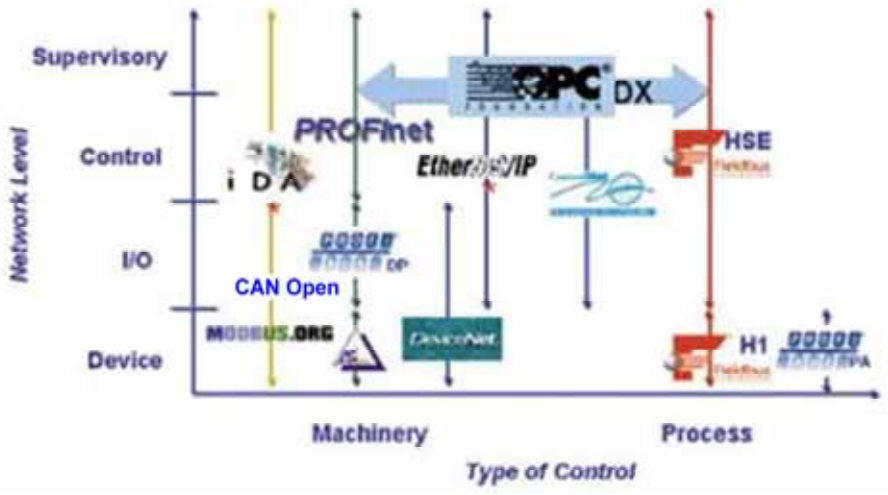
Acoplamiento Redundante

La utilización de switches redundantes permite establecer vínculos duplicados entre dos segmentos de red. Cuando se usa esta funcionalidad, combinada con la arquitectura de anillos se logra una alta confiabildad.

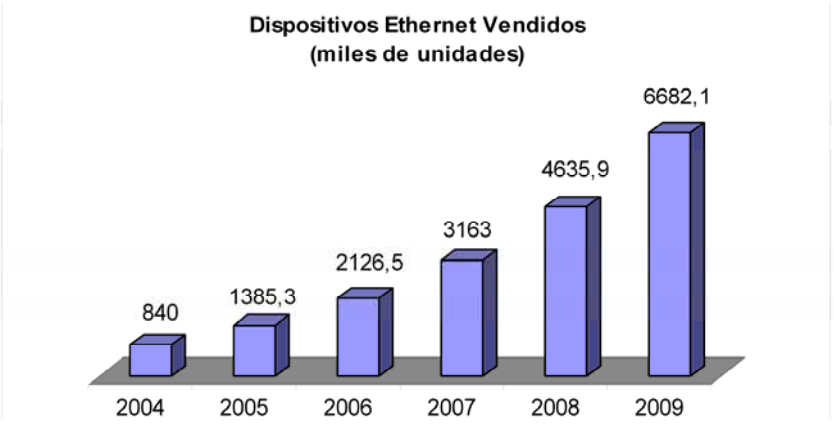
Protocolos de Capa de Aplicación



Del Dispositivo al SCADA

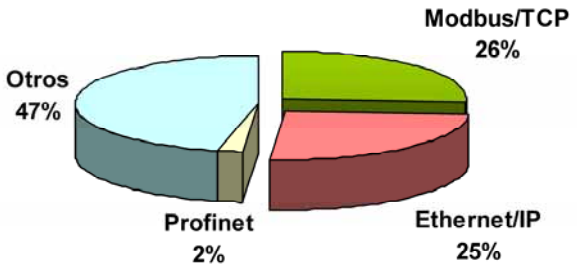


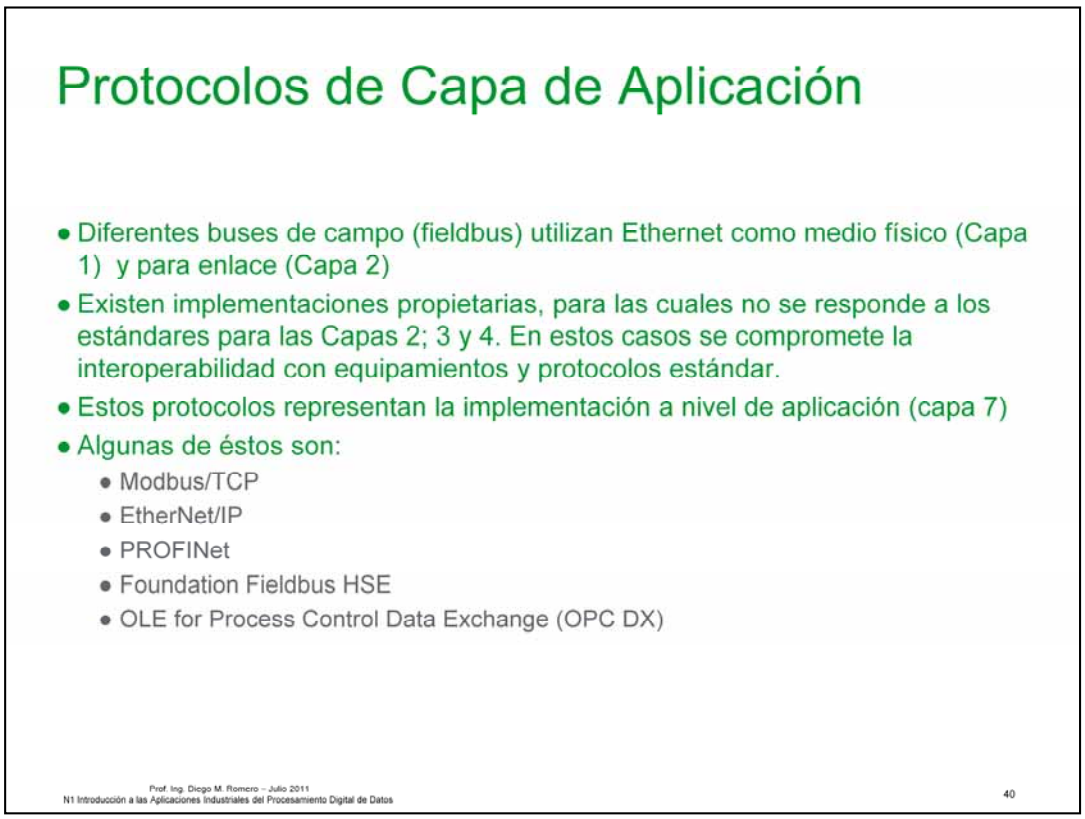
Algunas estadísticas



Algunas estadísticas

Dispostivos Ethernet Industriales por Protocolo
(Excluídos Switches)





Modelo de Interconexión de Sistemas Abiertos de 7 Capas (OSI, Open System Interconnection)

Capa 1 ~ Física

La Capa Física del modelo de referencia OSI es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico (cable de par trenzado, fibra óptica, radiofrecuencia, rayos infrarrojos, etc.); características del medio (p.e. tipo de cable o calidad del mismo; tipo de conectores normalizados o en su caso tipo de antena; etc.) y la forma en la que se transmite la información (codificación de señal, niveles de tensión/intensidad de corriente eléctrica, modulación, tasa binaria, etc.)

Capa 2 ~ Enlace de Datos

La capa de enlace de datos se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

Capa 3 ~ Red

La capa de red es la que se encarga de que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Provee el direccionamiento lógico, que utilizan los routers para definir dinámicamente los caminos de enlace entre orígen y destino.

Capa 4 ~ Transporte

Capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la destino, independizándolo del tipo de red física que se esté utilizando. Otra funcionalidad resuelta en esta capa permite que los paquetes sean entregados en el orden exacto en que se enviaron, asegurando una comunicación punto a punto libre de errores, o sin tener en cuenta el orden de envío.

Capa 5 ~ Sesión

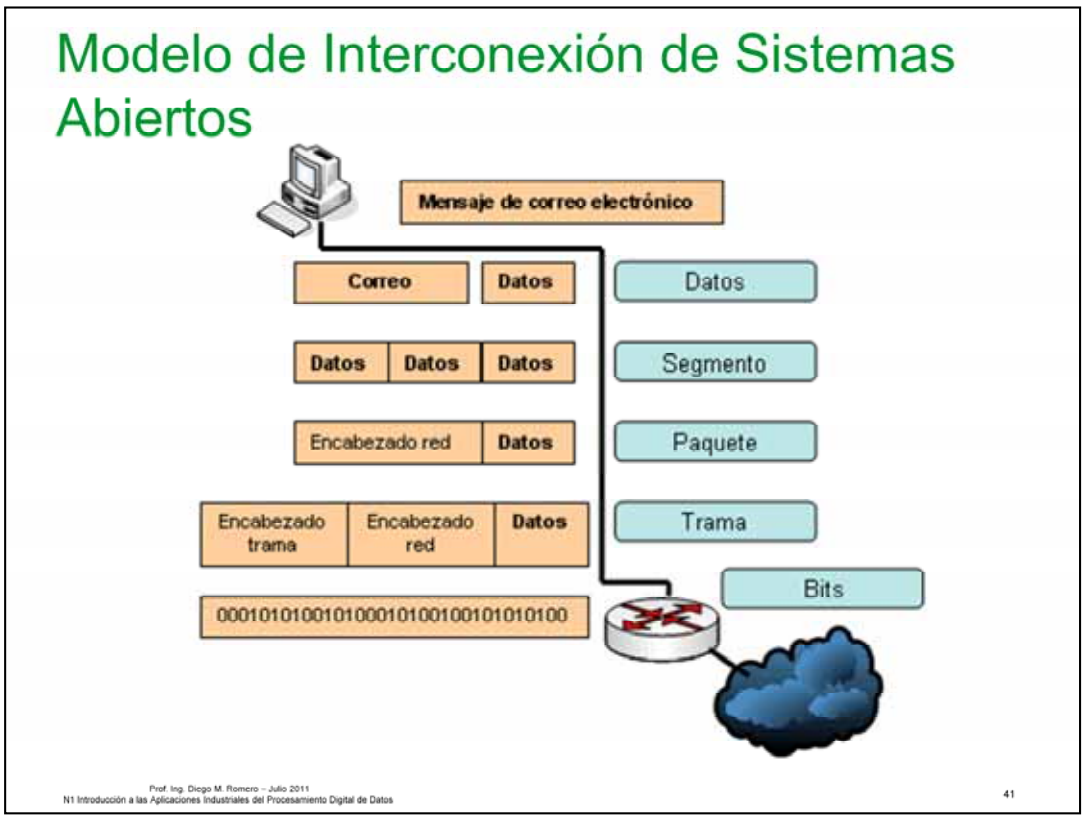
El servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcialmente, o incluso, totalmente prescindibles.

Capa 6 ~ Presentación

Es la encargada de manejar las estructuras de datos abstractas y realizar las conversiones de representación de datos necesarias para la correcta interpretación de los mismos. Permite que distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC), números (little-endian tipo Intel, big-endian tipo Motorola), sonido o imágenes pero que los datos lleguen de manera reconocible. Esta capa también permite también cifrar los datos y comprimirlos.

Capa 7 ~ Aplicación

Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos. Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar. El usuario normalmente no interactúa directamente con el nivel de aplicación, sino con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente.

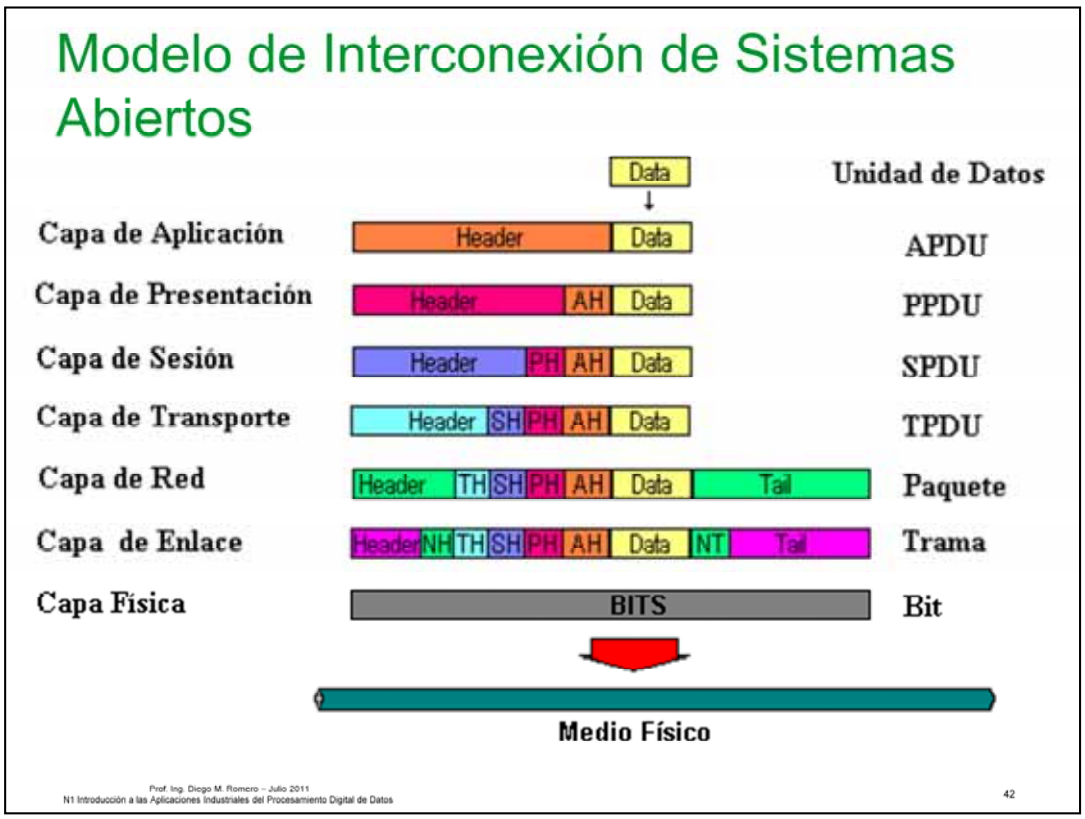


Transmisión de los datos

La capa de aplicación recibe el mensaje del usuario y le añade una cabecera constituyendo así la PDU (Unidad de datos de protocolo) de la capa de aplicación. La PDU se transfiere a la capa de aplicación del nodo destino, este elimina la cabecera y entrega el mensaje al usuario.

Para ello ha sido necesario todo este proceso:

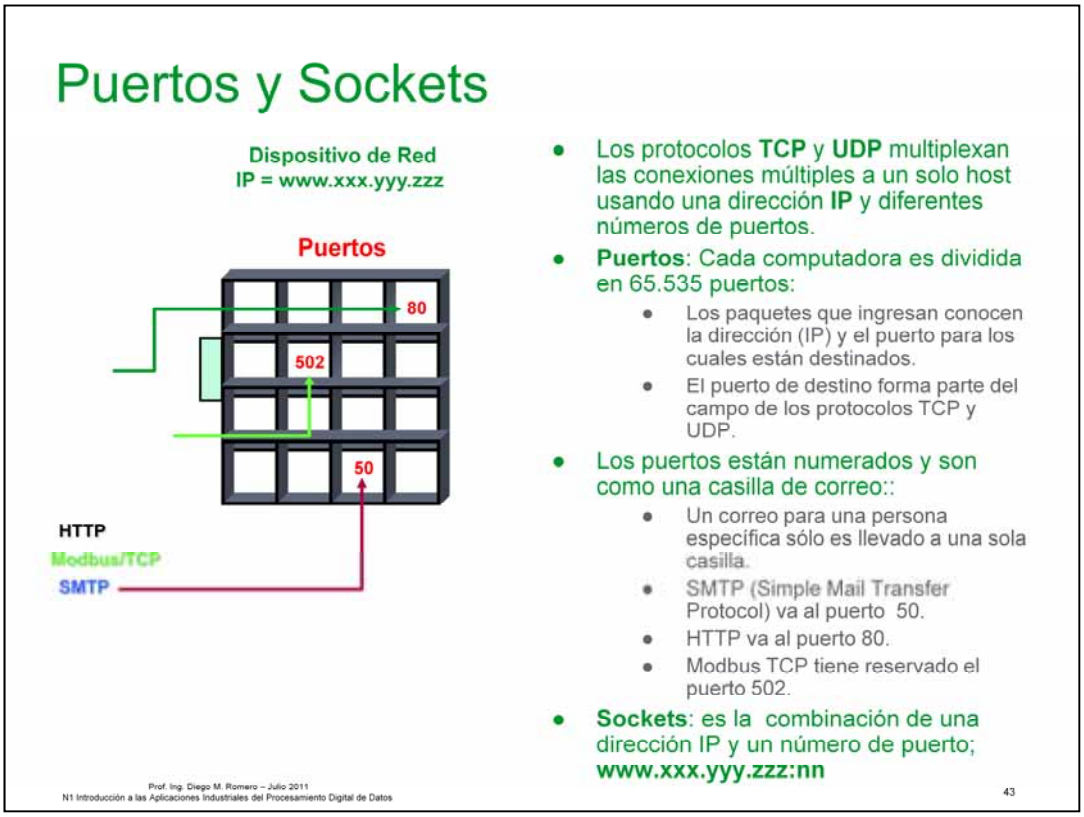
1. La PDU se pasa a la capa de presentación para ello hay que añadirla la correspondiente cabecera ICI (Información de control del interfase) y transformarla así en una IDU (Unidad de datos del interfase), la cual se transmite a dicha capa.
2. La capa de presentación recibe la IDU, le quita la cabecera y extrae la información, es decir, la SDU, a esta le añade su propia cabecera PCI (Información de control del protocolo) constituyendo así la PDU de la capa de presentación.
3. Esta PDU es transferida a su vez a la capa de sesión mediante el mismo proceso, repitiéndose así para todas las capas.
4. Al llegar al nivel físico se envían los datos que son recibidos por la capa física del receptor.
5. Cada capa del receptor se ocupa de extraer la cabecera, que anteriormente había añadido su capa homóloga, interpretarla y entregar la PDU a la capa superior.
6. Finalmente llegará a la capa de aplicación la cual entregará el mensaje al usuario.



Formato de los datos

Estos datos reciben una serie de nombres y formatos específicos en función de la capa en la que se encuentren, debido a como se describió anteriormente la adhesión de una serie de encabezados e información final. Los formatos de información son los siguientes:

- APDU ~ Unidad de datos en la Capa de aplicación
- PPDU ~ Unidad de datos en la Capa de presentación
- SPDU ~ Unidad de datos en la capa de sesión
- TPDU ~ Unidad de datos en la capa de transporte
- Paquete ~ Unidad de datos en el Nivel de red
- Trama ~ Unidad de datos en la capa de enlace
- Bits ~ Unidad de datos en la capa física



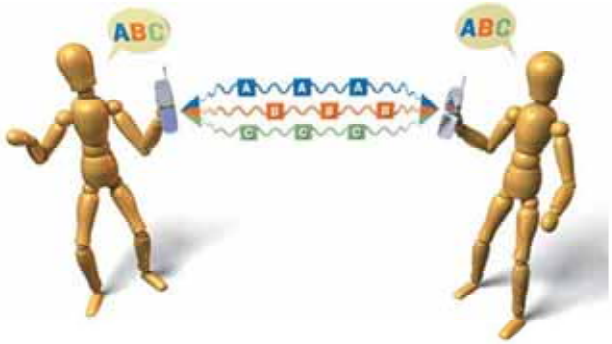
Un puerto puede verse como una casilla postal, donde se envía el correo de determinadas persona. Cada tipo específico de datos, procesados por determinadas aplicaciones, son direccionados a su puerto respectivo. Así por ejemplo la emulación de terminal Telnet utiliza el puerto 23; el protocolo para envío de correo electrónico (Simple Mail Transfer Protocol ó SMTP) se dirige al puerto 25; la transferencia de páginas WEB con el protocolo HTTP tiene asignado el puerto 80 y para el protocolo Modbus/TCP se ha reservado el puerto 502. Cada secuencia de tramas TCP, correspondiente a una determinada aplicación, se define por la dirección IP del dispositivo de destino (host) y por el puerto asignado en éste para aquella. En el host de destino la combinación de dirección IP propio y puerto TCP se denomina **socket**, único para cada aplicación.

Cuando una secuencia de tramas es iniciada en un host, éste determina un puerto propio libre y el puerto en el host remoto con el cual se debe establecer la conexión, según la aplicación de destino. Por ejemplo en una sesión FTP, el que la inicia podría elegir el puerto 1025 para recibir la respuesta (listen port) y el puerto 21 para comunicarse (talk port) con el host remoto (puerto de destino predeterminado para el protocolo FTP). El puerto para recibir la respuesta es generalmente determinado por el sistema operativo, puede variar con cada nueva secuencia de tramas, ya la aplicación no tiene control sobre tal elección. Al responder, el host remoto utiliza ese puerto para identificar cada trama de respuesta.

Servicios de red

- Es posible combinar en una misma red Ethernet y en los dispositivos de automatización los servicios para aplicaciones de oficina e industriales:
  - Mensajería Modbus/TCP ó Ethernet/IP
  - Servicios WEB (HTTP)
  - Correo electrónico (SMTP)
  - Transferencia de archivos (FTP y TFTP)
  - Asignación dinámica de direcciones IP (DHCP cliente y servidor)
  - Reemplazo de dispositivos dañados (Opción 82 DHCP y TFTP)
  - Sincronismo de hora y fecha (NTP / SNTP / PTP)
  - Administración remota de dispositivos de red (SNMP)
  - Supervisión remota (RMON)

Conectividad inalámbrica



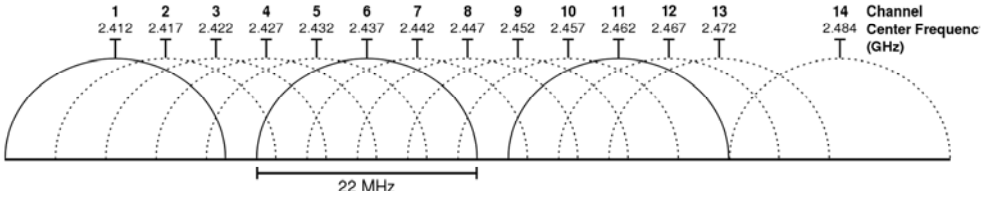
© BRYAN CHRISTIE; IEEE Spectrum March 2004

Algunos conceptos en WiFi

Canales y Frecuencias

802.11b/g

- Una única banda de frecuencia: 2,4 GHz
- 14 canales definidos
- 11 canales no licenciables (US, EU, Jap, AR)
- Ancho de cada canal +/-11MHz
- Sólo hay 3 canales que no se superponen

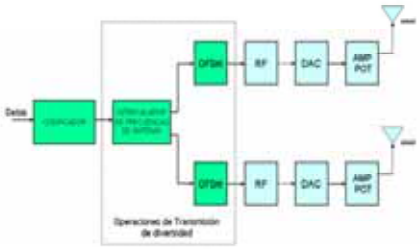


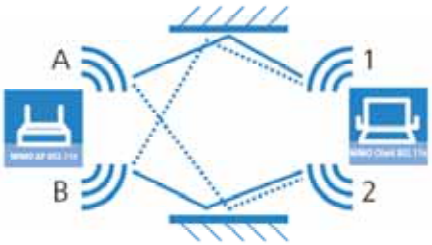
Algunos conceptos en WiFi

Canales y Frecuencias

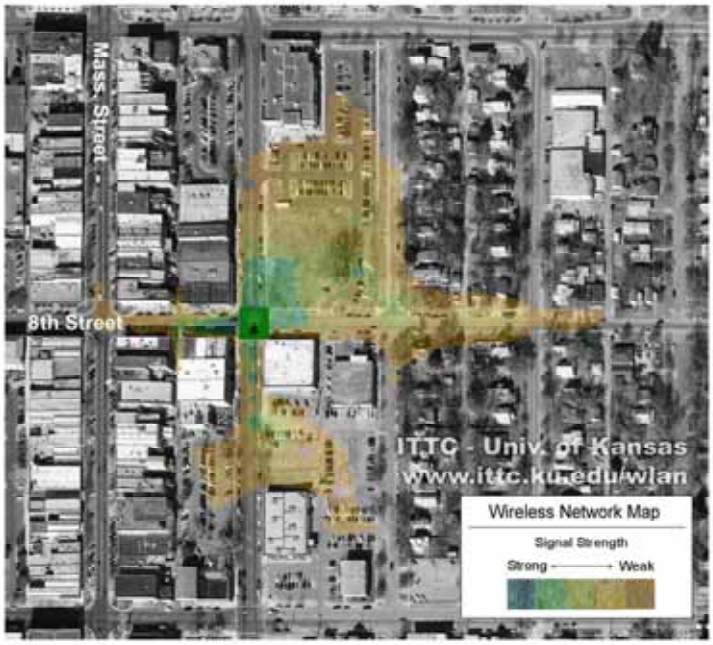
802.11n

- 4 bandas de frecuencias : 5,1GHz; 5,3 GHz; 5,4GHz y 5,8 GHz
- 24 canales definidos
- Sólo 5 canales permitidos para espacios abiertos con modulación DFS y TPC para evitar interferencias
- Ancho de canal 20 MHz ó 40 MHz para velocidades mayores
- Tecnología MIMO (Multiple Input Multiple Output) de antenas múltiples





Algunos conceptos en WiFi



- WiFi = Señales de radio
- Comportamiento dificil de predecir
- Requiere una planificación cuidadosa

Estándar 802.11

Cuadro Comparativo

Estándar / Caracter.	IEEE 802.11a	IEEE 802.11n	IEEE 802.11b	IEEE 802.11g
Banda Frecuencia	5 GHz (no licenciada)	2,4 / 5 GHz (no licenciada)	2,4 GHz (no licenciada)	
Nro. Canales	Hasta 24 no interferridos entre si		11; sólo 3 no superpuestos	
Potencia (E.I.R.P.)	Interior hasta 23 dBm (200mW) Exterior hasta 30dBm (1000mW)		Máxima 20dBm (100 mW)	
Ancho de Banda Máximo	54 Mbit/s	300 Mbit/s	11 Mbit/s	54 Mbit/s
Ventajas	Alta velocidad,, potencia elevada, canales múltiples, banda con baja interferencia	Alta velocidad, compatible, con otros estándares, mayor alcance, tecnología MIMO para múltiples conexiones por canal	Alta disponiblidad de productos	Alta velocidad, compatible con IEEE 802.11b, alta disponibiliad de productos
Desventajas	No compatible con IEEE 802.11g/b, mayor atenuación a igualdad de condiciones de propagación	Estándar reciente, baja disponiblidad de productos	Baja velocidad, banda muy utilizada (Bluetooth, hornos microondas, etc.), potencia de salida limitada	Banda muy utilizada (Bluetooth, hornos microondas, etc.), potencia de salida limitada, menor velocidad en operación compatiblle con IEEE 802.11b

•Hace uso de la tecnología “spread spectrum” para las comunicaciones

•Se comparte un medio común, creando “dominios de colisiones”

•Permite la conexión en red de dispositivos portátiles (notebooks, PDAs, Tablet PCs, teléfonos VoIP, etc.)

•Facilita la instalación de nuevas redes en edificios que no cuentan con la infraestructura adecuada.

•Permite el acceso a Internet en lugares públicos (“hotspots” en aeropuertos, cyber cafés, restaurantes, bibliotecas, hoteles, universidades, etc.)

E.I.R.P.: Equivalent isotropically radiated power (Potencia equivalente irradiada isotrópicamente)

$E.I.R.P. = P_T - L_C + G_A$

P_T : Potencia de salida del transmisor (dBm)

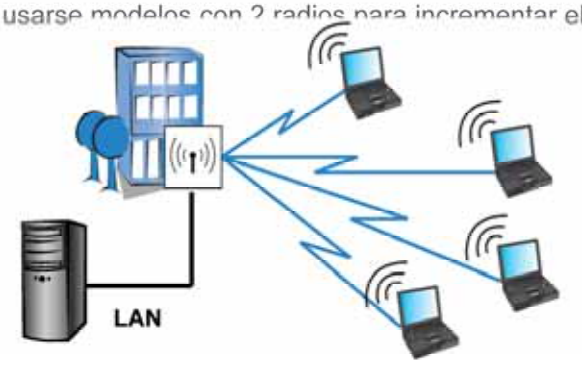
L_C : Atenuación del cable (dB)

G_A: Ganancia de antena con respecto a antena isotrópica ideal (dBi)

Architecturas WiFi

Punto de Acceso Simple

- El Punto de Acceso (Access Point) provee a los dispositivos clientes inalámbricos un punto de conexión a la red local cableada (LAN)
  - Los clientes pueden ser de diferentes fabricantes y estándares, 802.11 a/b/g/n
  - Pueden usarse modelos con 2 radios para incrementar el ancho de banda

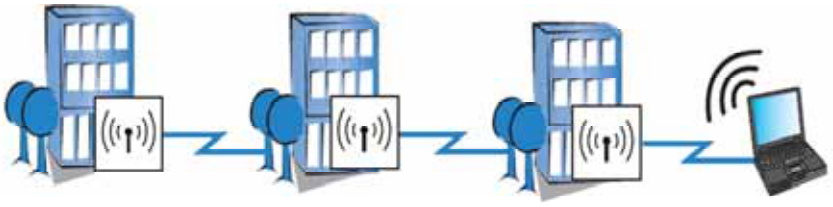


Arquitectura WiFi
Bridge Punto a Punto

- Los Puntos de Acceso permiten una configitación en modo bridge punto a punto
  - Dos dispositivos WiFi proveen un enlace de comunicación punto a punto para vincular entre si dos redes locales cableadas
  - Modelos con 2 radios pueden ser usados para crear vínculos redundantes

Arquitectura WiFi
Bridge con Relevo

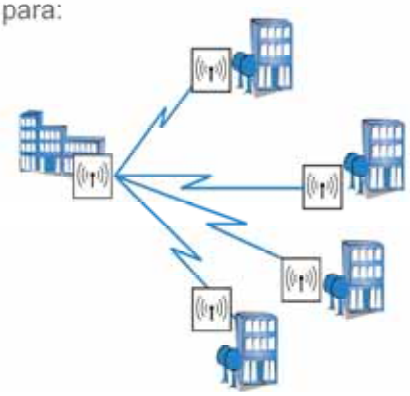
- El Punto de Acceso opera como repetidor, retransmitiendo las señales de radio, ampliando el alcance
  - Uno o más dispositvos WiFi de dobe radios funcionan como estaciones de relevo de mensajes, proveyendo vínculos de comunicación entre dos o tres redes locales cableadas



Arquitectura WiFi

Punto de Distribución

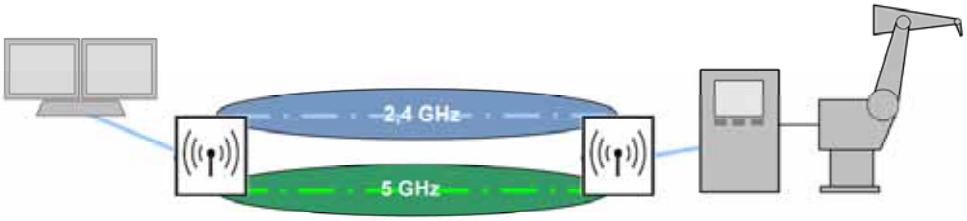
- Un dispositivo WiFi maestro conecta multiples puntos de acceso esclavos a una red local cableada, en una topología punto a multipunto
  - Pueden usarse modeloss con 2 radios para:
    - Incrementar el ancho de banda
    - Vínculo redundante standby



Arquitectura WiFi

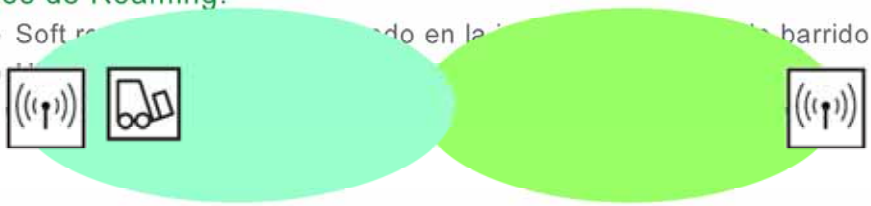
Red Inalámbrica Redundante

- Dos interfaces de radio en el punto de acceso
  - Dos rangos de frecuencias posibles



Arquitectura WiFi
Roaming

- El roaming le permite al cliente moverse entre puntos de acceso distintos
- Las estaciones cliente pueden moverse y acceder a cada punto de acceso, independientemente del canal, si se cumple con estos requisitos:
  - Todos los puntos de acceso deben usar el mismo SSID
  - Todos los puntos de acceso deben tener la misma configuración de segurdiad
- Tipos de Roaming:
  - Soft r… …do en la … … barrido
  -



La reducción del costo de las instalaciones de la planta: el cableado del sitio en plantas de proceso, fábricas y edificios todavía representan un costo importante en un proyecto de automatización. Utilizando conectividad inalámbrica para reducir o eliminar gran parte de esto es obviamente atractivo donde puedan implementar. De esta forma se logra mejorar la comunicación entre dispositivos sin el costo adicional del cableado.

La norma 802.11 define el Wired Equivalent Privacy (WEP):

Encriptación propia de las normas IEEE 802.11

Basada en algoritmo RC4, con clave simétrica y estática (de 40 ó 128 bits)

La clave se ingresa manualmente en “Clientes Inalámbricos” y “Access Points”

En determinadas condiciones la contraseña de acceso viaja sin encriptar

Debilidades:

- No asegura la privacidad.
- No bloquea el acceso no autorizado a la red de la cual el Access Point forma parte
- No impide que un cliente inalámbrico legítimo se conecte a un Access Point no autorizado (Rouge Access Point)
- Se ve comprometida ante la pérdida de algún dispositivo con la clave configurada

Mejorando la seguridad

Usar esquemas de seguridad a Nivel de Capa 2 (MAC address) o de Capa 3 (IP Security).

Implementar Redes Privadas Virtuales (VPN) con “Remote Authentication Dial-In User Service (RADIUS)”:

- Autenticación basada por Usuario (ID + Contraseña).
- Administración centralizada de credenciales.

Uso de algoritmos de encriptación con claves dinámicas (por sesión).

Mecanismos de autenticación mutua de dispositivos (impide que un cliente inalámbrico sea engañado por un Access Point no autorizado).

Uso de algoritmos de encriptación a Nivel de Aplicación (Capa 7).

SSID múltiples

¿Y la seguridad en WiFi…?
Comparando opciones

	WEP	WPA	802.11i
Encriptación	Claves sencillas, fáciles de descubrir	Utiliza para encriptar los protocolos TKIP y MIC Muy baja probabilidad de repetición de claves	Seguridad equivalente a VPN con AES
Algoritmo	40 bit; 104 bit y 128 bit RC4	128 bit RC4 (TKIP)	128 bit AES
Generación de Claves	Distribución manual, permite ataques de tipo "man-in-the-middle"	Automática, a partir de palabra inicial "keyphrase"	Automática, protocolo AES en hardware
Autenticación	Clave transferida inicialmente como texto plano sobre el vínculo	Intercambio de clave siempre encriptado	Intercambio de clave siempre encriptado

TKIP: Temporal **K**ey **I**ntegrity **P**rotocol

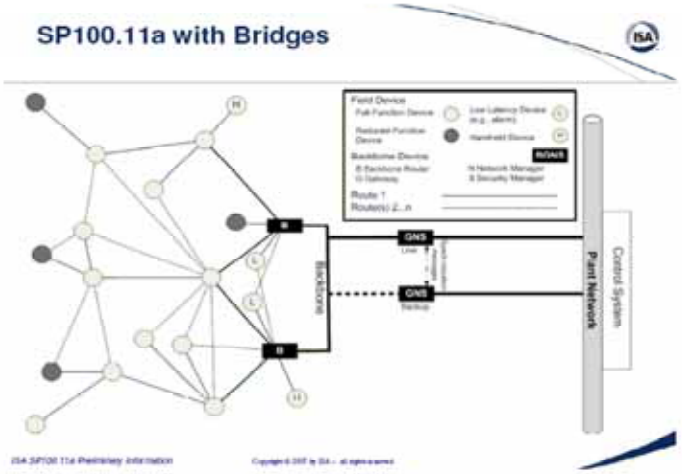
MIC: Message **I**ntegrity **C**ode

AES: Advanced **E**ncryption **S**tandard

Norma ISA SP100.11a

- Elaborada por la Comisión 100 de la ISA (Instrument Society of America), cuyos objetivos son:
  - Definir el entorno de operación de una red inalámbrica orientada a dispositivos de campo
  - Identificar y definir las tecnologías a utilizar
  - Identificar las aplicaciones
- El estándar especifica las siguientes funciones:
  - Suite de protocolos:
    - Capa física basada en el estándar IEEE 802.15.4-2006 con salto de frecuencia de banda angosta (ZigBee)
    - IPv6 over Low power WPAN (6lowpan) de Internet Engineering Task Force (IETF)
    - Topología mesh basada en estándar (draft) IEEE 802.11s
    - EDDL (IEC 61804-3)
  - Definición de enlaces
  - Seguridad
- Última revisión aprobada en abril de 2009

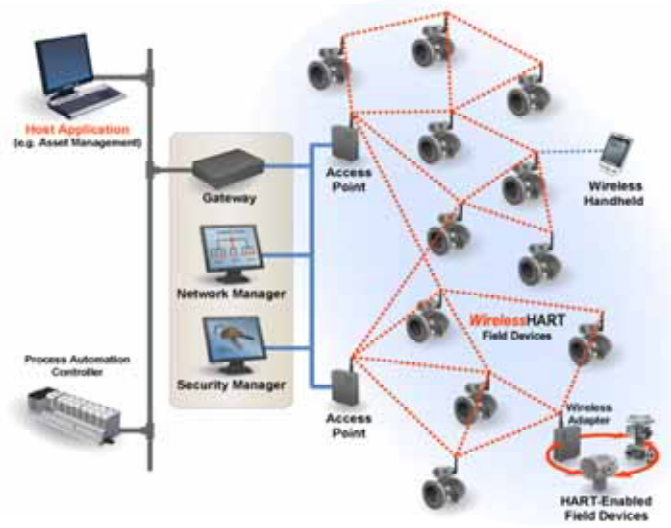
Norma ISA SP100.11a



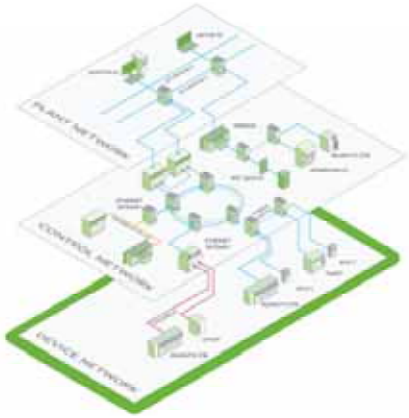
*Wireless*HART

- Publicado en 2007 por HART Communications Foundation (HCF)
- Aprobada por el Comité Europeo de Normalización (CEN) y por la Comisión Electrotécnica Internacional (IEC) como estándar IEC 62591 Edición 1.0 en 2009
- Basada en estándares internacionales:
  - Protocolo HART (IEC 61158)
  - EDDL (IEC 61804-3)
  - "Spread Spectrum"; basada en salto de frecuencia de banda angosta y estándar) IEEE 802.15.4 y topología mesh

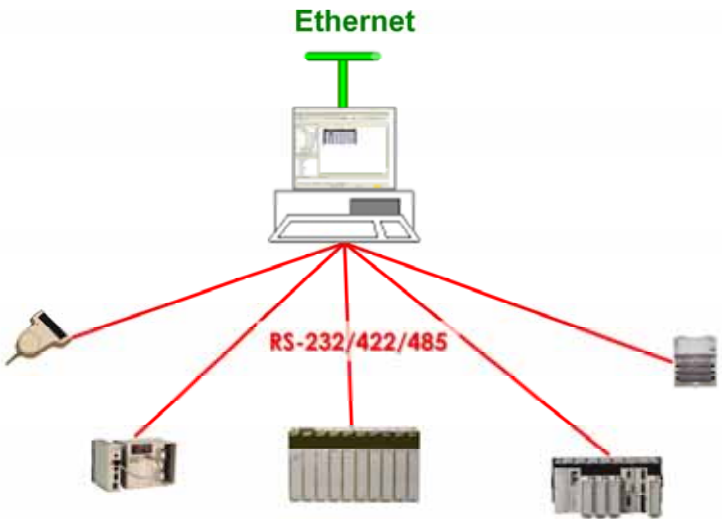
WirelessHART



Conversores Serie a Ethernet



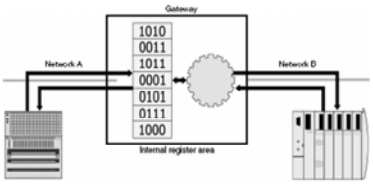
Topología Serie Punto a Punto



Bridge Serie – Ethernet

Memoria Compartida

- Se basan en una zona de memoria compartida donde se almacenan los datos de planta.
- El intercambio de datos es realizado por medio de la lectura/escritura de esos valores.
- El lado serie se configura para interrogar los dispositivos.



Prof. Ing. Diego M. Romero – Julio 2011
N1 Introducción a las Aplicaciones Industriales del Procesamiento Digital de Datos

78

Ventajas:

- La respuesta del lado Ethernet es rápida (los datos se leen de la memoria compartida y no son afectados por el retardo de respuesta de los dispositivos serie).
- El tiempo de respuesta no se ve afectado por fallas en los dispositivos serie.
- Pueden usarse diferentes protocolos a cada lado del bridge.

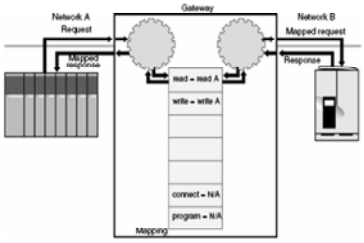
Desventajas:

- No permite utilizar comandos de programación.
- Acceso limitado a los tipos de datos definidos en la memoria compartida.
- Puede dar una idea errónea del desempeño del sistema

Bridge Serie – Ethernet

Conversión de Protocolo

- Opera recibiendo una interrogación de una red y la convierte a otra compatible con la segunda.
- La conversión de las consultas la define el diseñador (tipo consulta A = tipo consulta B).



Ventajas:

- Permite utilizar diferentes protocolos a cada uno de los lados del bridge.

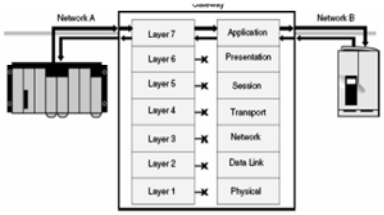
Desventajas:

- No permiten el pasaje de comandos de programación, ya que son diferentes para cada uno de los protocolos.
- Acceso limitado a aquellos tipos de datos comunes a ambas redes.
- Acceso limitado a aquellos consultas definidas por el diseñador del bridge.
- Menor velocidad de respuesta del lado Ethernet dado que los comandos deben pasar al lado serie, procesados por los dispositivos y respondidos antes de devolverlos a su origen.

Bridge Serie – Ethernet

"Pass Through"

- El bridge recibe una comando desde una de las redes y reenvía el mismo comando a la otra.
- No se requiere realizar conversión alguna ya que el protocolo de aplicación es el mismo para ambas redes.



Prof. Ing. Diego M. Romero – Julio 2011
N1 Introducción a las Aplicaciones Industriales del Procesamiento Digital de Datos

80

Ventajas:

- Permite el uso de cualquier código de función del protocolo de aplicación, incluyendo la programación y la actualización de firmware.

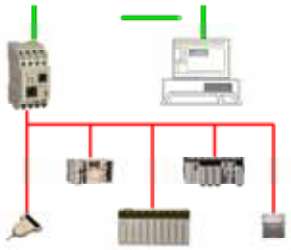
Desventajas:

- Menor tiempo de respuesta del lado Ethernet ya que los comandos deben ser pasados al lado serie y respondidos antes de ser devueltos al origen.
- Los tiempos de respuesta del lado Ethernet son afectados por la falla de dispositivos del lado serie.

Bridge Serie – Ethernet

Conexión Serie Virtual

- El protocolo serie es encapsulado en tramas Ethernet, transmitido al bridge y nuevamente convertido a su formato original en éste.
- Existen diferentes modos de funcionamiento:
  - Por sockets TCP ó UDP, donde el bridge se comporta como un servidor o un cliente. Puede ser usado para conectar un host (normalmente una PC) con un dispositivo serie o dos bridges entre si.
  - Redirector de puerto serie, cuando el bridge es visto desde el host (normalmente una PC), como un puerto serie virtual.



Ventajas:

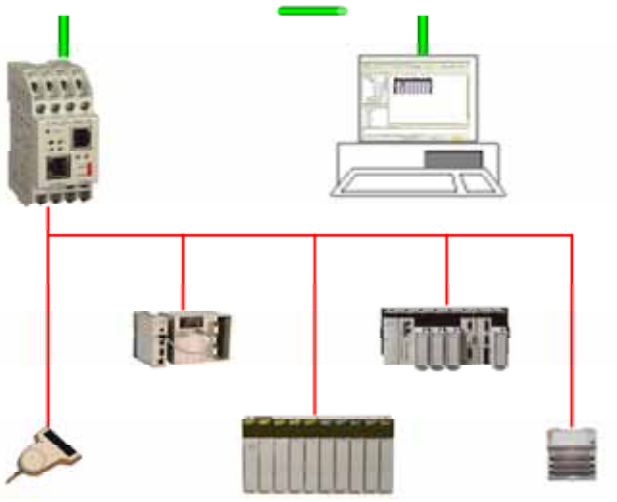
- Permite la conexión de dispositivos serie entre si aprovechando la infraestructura Ethernet existente.

Desventajas:

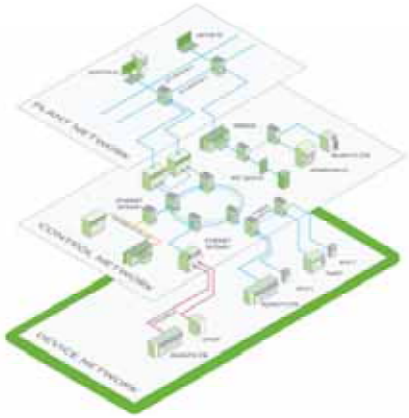
- Requiere el desarrollo de aplicaciones específicas en el host (por sockets) o la instalación de un controlador de dispositivo (redirector).
- Soluciones propietarias de cada fabricante

Bridge Serie – Ethernet

Conexión Serie Virtual



Conversores de medio físico



Cable de Fibra Óptica

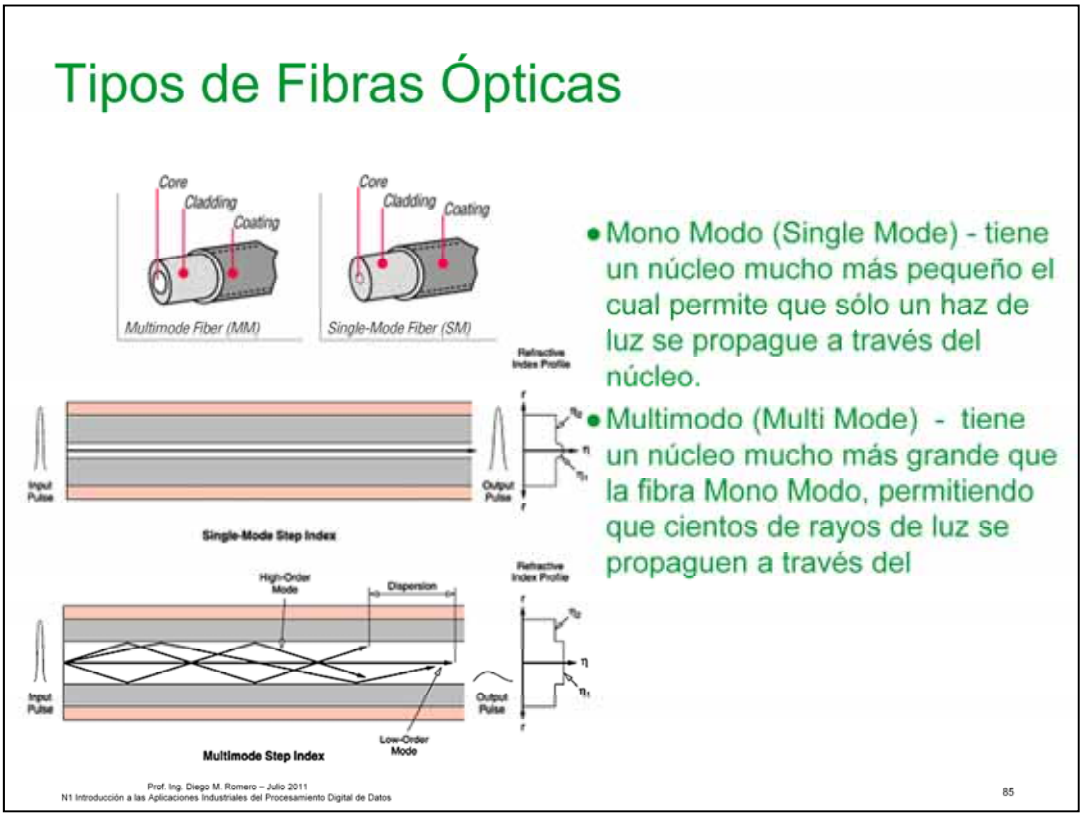
- Consiste de tres partes :
  - **Núcleo :** de vidrio o plástico, provee un canal para el haz de luz
  - **Cobertura (Cladding) :** cilíndrico concéntrico al núcleo que refleja por refracción total cualquier rayo de luz hacia el núcleo
  - **Vaina de Protección :** elemento externo que brinda protección al núcleo y a la cobertura
- La fibra óptica es inmune a la interferencia y permite mayores extensiones de segmento (2 km con multimodo ó 20 km con monomodo)
- A menudo usado como vínculo troncal

Prof. Ing. Diego M. Romero – Julio 2011
N1 Introducción a las Aplicaciones Industriales del Procesamiento Digital de Datos

84

Los cables de Fibra Óptica son la elección indicada para aquellos enlaces que involucren altas velocidades de transmisión y grandes volúmenes de información [video, bases de datos], distancias grandes o interconexión de sitios. Si bien ha disminuido en los últimos años, su costo sigue siendo mayor que los cables de cobre (pares retorcidos o coaxil), y requiere conectores y herramientas de empalme específicas.

Las características de los cables de fibra óptica cable los hacen indicados para redes troncales, vinculando entre si dos o más LANs y anillos redundantes (FDDI rings). Pueden operar a velocidades de 100 Mbps ó 1 Gbps, son totalmente inmunes a la interferencia electromagnética y a la posibilidad de capturas clandestinas de información.



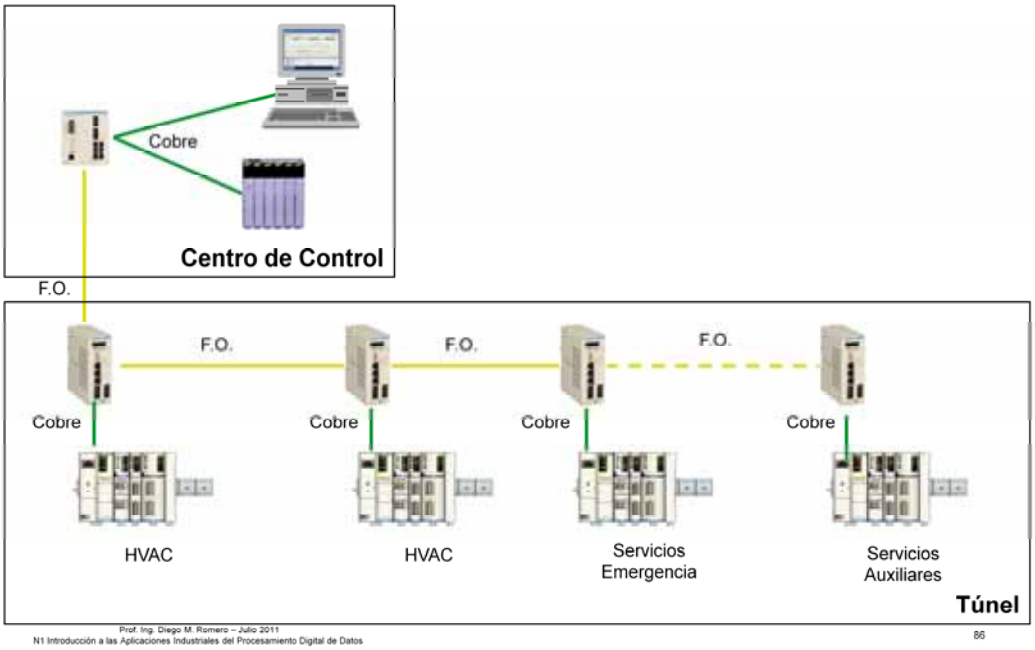
Las diferencias entre los dos tipos de fibra óptica se encuentran en el tamaño y características ópticas de los núcleos (la región de la fibra por donde viaja la luz). La fibra **MultiModo** tiene un diámetro mayor y su índice de refracción varía en forma gradual desde el centro hacia la periferia. Los cables de fibra multimodo tienen un diámetro en el rango de 50 a 100 μm (un micrón, μm, es la 1/25 parte del diámetro de un cabello humano). Cada fibra multimodo es capaz de transportar una señal determinada. Su mayor diámetro de núcleo facilita la interconexión y por su atenuación limita el alcance a 2.000 metros.

La fibra **MonoModo** se construye con un núcleo de diámetro mucho menor e índice de refracción uniforme, con lo cual la luz se propaga en un único modo. Los cables de fibra monomodo presentan un ancho de banda mayor y menor atenuación que las multimodo. El diámetro del núcleo varía entre 8 y 10 μm. La interconexión requiere mayor precisión pero su menor atenuación permite llegar a enlaces de hasta 20.000 metros, con mayor ancho de banda.

En cualquier aplicación que incluya fibra óptica, requiere realizar un cálculo de atenuaciones, incluyendo los conectores, empalmes y derivaciones. De dichos cálculos surge la distancia máxima que podrá cubrirse utilizando un determinado tipo de fibra óptica.

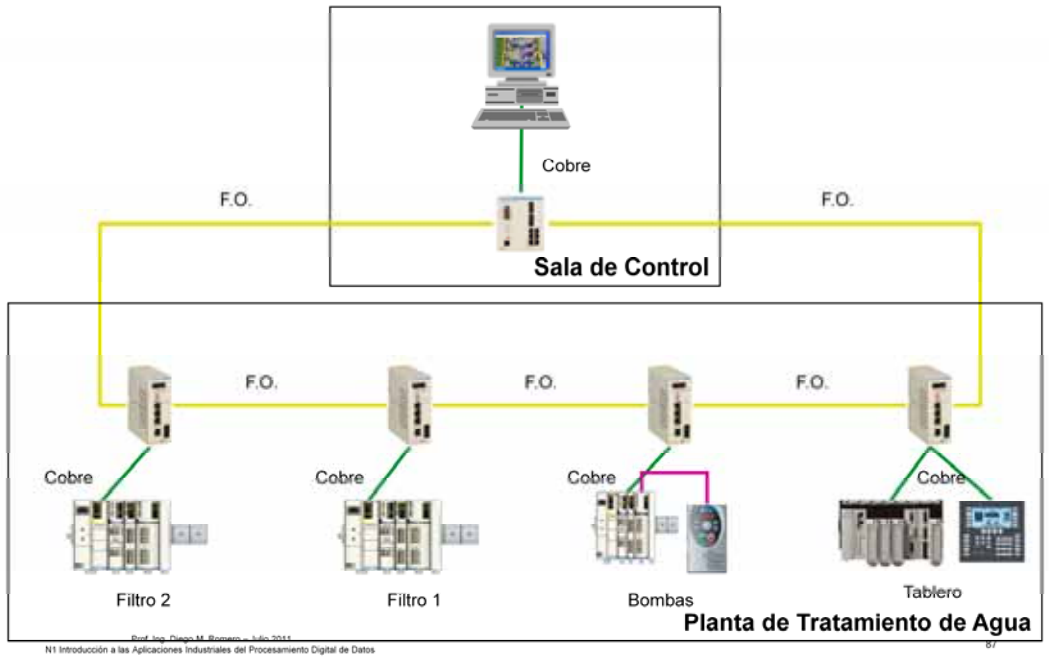
Aplicaciones de Fibra Óptica

Grandes Distancias

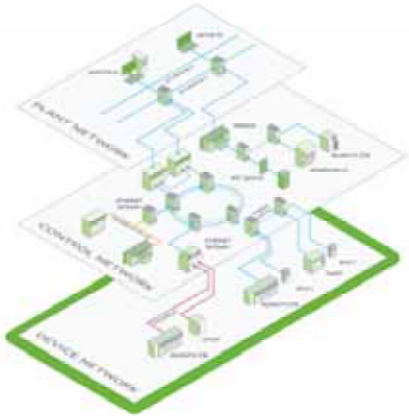


Aplicaciones de Fibra Óptica

Confiabilidad y Disponibilidad



Bibliografía



Referencias y Bibliografía

- http://www.ieee.org/
- http://standards.ieee.org/wireless/
- http://www.isa.org/
- http://www.aadeca.org/
- http://www.iec.ch/
- http://www.modbus-ida.org/
- http://www.odva.org
- http://www.hartcomm.org/
- http://ietf.org/
- http://www.ethernet-ip.org/
- http://www.opcfoundation.org/
- http://www.fieldbus.org/
- http://www.profibus.com/
- http://www.automation.com
- http://www.automatas.org/
- http://www.controlglobal.com
- http://www.control.com/
- http://www.plcs.net
- http://www.plcopen.org
- http://ethernet.industrial-networking.com/
- http://www.bitpipe.com
- http://www.ethereal.com

- EtherNet/IP™ - CIP on Ethernet Technology. ODVA. Ann Arbor, Michigan, U.S.A. 2006.
- Piedrafita Moreno, Ramón. Ingeniería de la Automatización Industrial. Editorial Ra-Ma. Madrid. 2003.
- Rio, Ralph Rio; Forber, Harry; Polsonetti, Chantal. Industrial Ethernet Worldwide Outlook – Market Analysis and Forecast 2005 ~ 2009. ARC Advisory Group. Dedham MA U.S.A. 2005
- Ethernet Industrial para todos los gustos. Revista Instrumentación y Control Automático. Editorial Soluciones en Control S.R.L. Año 32; N° 131.
- Craig Mathais, Farpoint Group. Broadband Everywhere: Putting Mobile Data to Work. 2005. http://www.networkworld.com/resources/wirelessandmobility/presentations/keynotemorning.pdf
- Caro, Dick ~ CMC Associates. Wireless industrial standard ISA SP100.11a. ControlGlobal.com. Abril 2007.
- Estándares wireless: ¿Dónde estamos?. Revista Instrumentación y Control Automático. Editorial Soluciones en Control S.R.L. Año 36; N° 151.

¡Muchas gracias...!

diego.romero@schneider-electric.com