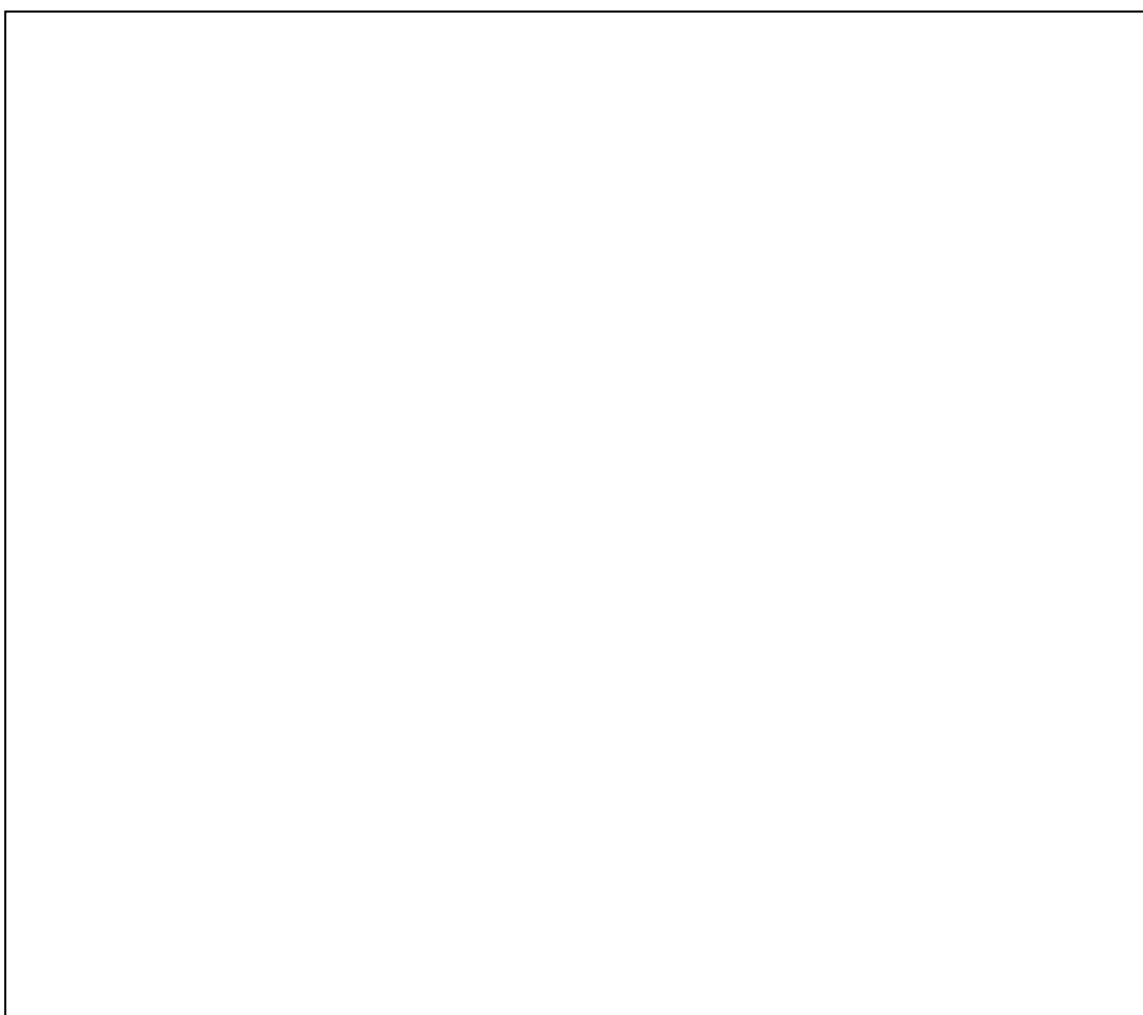


Introducción a Ethernet Industrial

Algunos conceptos

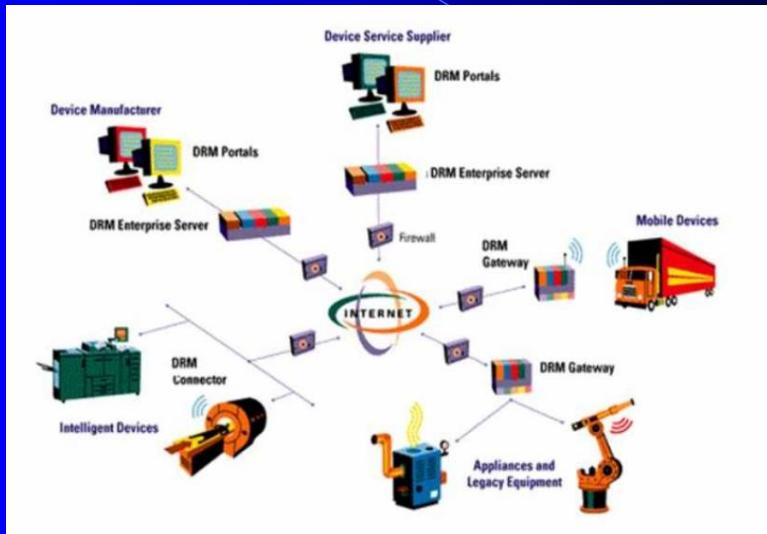
Prof. Ing. Diego M. Romero
Octubre 2005



Contenido

- ❖ Requerimientos de las redes Ethernet para aplicaciones industriales
- ❖ Switches Ethernet para aplicaciones de piso de planta
- ❖ Conectividad inalámbrica en ámbitos industriales
- ❖ Conversores Serie a Ethernet
- ❖ Conversores de medio físico
- ❖ Referencias

¿Qué es una Red Industrial?



Introducción a Ethernet Industrial



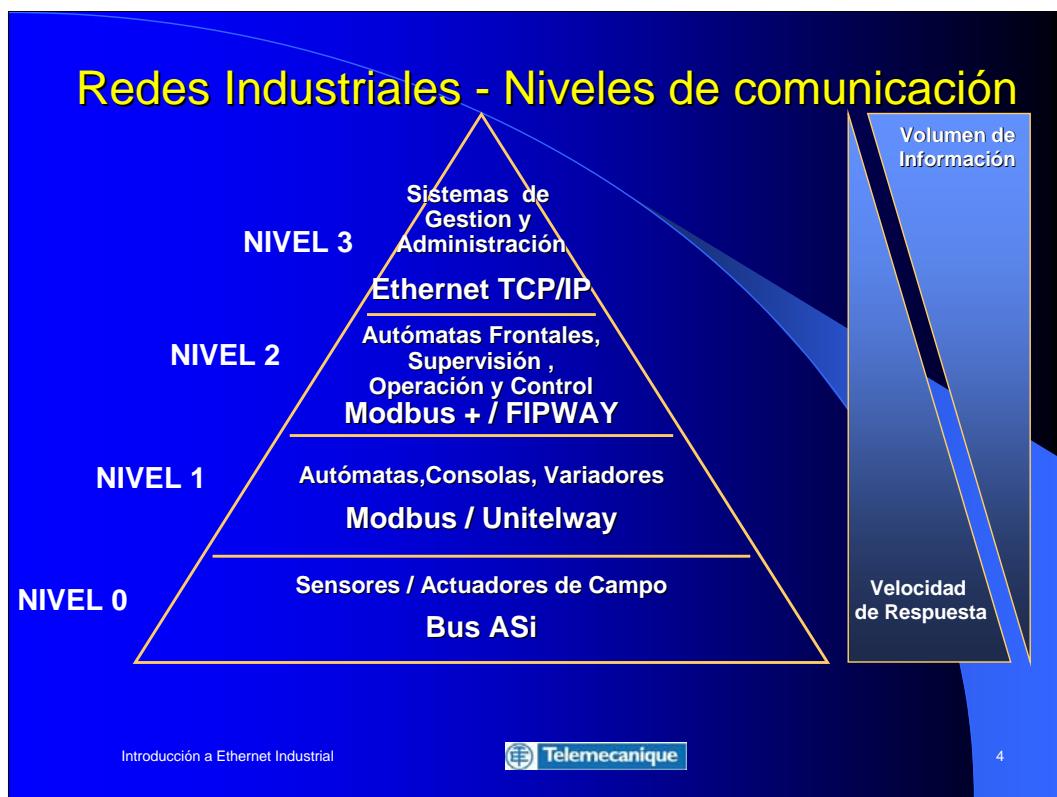
3

Ethernet, which has seen great success and received universal acceptance in corporate and university offices, has begun to find its way into the more demanding industrial environment. The attractions of Ethernet include the ability to monitor data transmissions, the existence of utilities (such as Telnet) which are used to set up and reconfigure equipment, and the capability to load control device programs from a central location. These types of applications are often referred to as "at the management level," although there is a move afoot to adopt Ethernet "at the device level," too. This includes using TCP/IP Ethernet connections to transmit control signals, such as in robotics, the operation of high-speed sorting equipment, and SCADA (Supervisory Control And Data Acquisition) applications.

Evolución de las redes industriales propietarias.

Integración de la información de piso de planta con los sistemas de gestión (MRP/ERP).

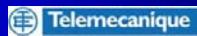
Ampliar la conectividad por medio de Internet.



Confiabilidad, velocidad y seguridad de operación

- ❖ Acceso determinístico al medio.
- ❖ Mayor confiabilidad para las aplicaciones industriales, que la ofrecida por los productos habitualmente usados en aplicaciones para oficina u hogar.
- ❖ Ambientes industriales con condiciones desfavorables:
 - ❖ Temperaturas extremas.
 - ❖ Operación con diferentes tensiones de alimentación, tanto en CC como en CA.
 - ❖ Ruido eléctrico y transitorios.
 - ❖ Atmósferas agresivas y condiciones de uso extremas.
- ❖ Recuperación rápida ante fallas y seguridad, que ayude a una operación continua (24 x 7) y segura en el ambiente industrial.
- ❖ Uso de fibra óptica.

Introducción a Ethernet Industrial



5

As Ethernet moves from the office to the factory floor, it is important to keep in mind that the purpose of commercially available network equipment, such as an Ethernet switch, is for connecting PCs, printer servers, and other devices that are designed to work in the comfort of offices and climate-controlled corporate machine rooms. This means that if you purchase Ethernet equipment that was originally designed for office applications, but then use the equipment in your demanding industrial environment, you run the risk of causing tremendous damage to your industrial system. Because each industrial device, such as a PLC, is networked, the device plays a very important role when it comes to the operation of the entire industrial system. This is unlike the average office application, in which the failure of Ethernet equipment might merely mean that a few PCs cannot send e-mail messages for a couple of minutes.

But in the industrial application, when an industrial device loses its connection to the network, the result could be a huge financial loss.

When choosing Ethernet equipment to fulfill the requirements of industrial applications, and to ensure that your entire industrial system keeps running smoothly, you should keep the following points in mind.

Conectividad y facilidad de uso

- ❖ Fácil Instalación y Mantenimiento:
 - ❖ 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.
- ❖ Equipos existentes sin conectividad a Ethernet.
- ❖ Necesidad de asegurar los datos.
- ❖ Protocolos de “Capa de Aplicación”.

Acceso determinístico

♦ Ethernet es, por su diseño original:

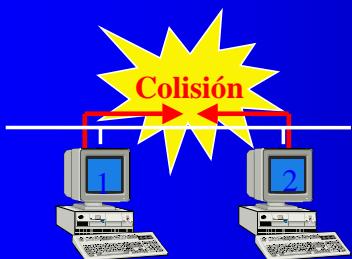
- ♦ No determinística.
- ♦ Topología bus (física y/o lógica).
- ♦ Half duplex.
- ♦ El dispositivo de menor velocidad determina la de todo el bus.
- ♦ Los dispositivos conectados al bus “ven” las colisiones de toda la red.

As specified originally, Ethernet was half-duplex and existed on a bus topology, which meant that some type of “collision detection and avoidance” mechanism (the technical term for this is CSMA/CD, or *Carrier Sense Multiple Access with Collision Detection*) needed to be built into the specification, resulting in a “non-deterministic” data transmission interface. It was certainly a far cry from the simpler and more familiar RS-232 interface, and is one reason that Ethernet was eschewed by the industrial control community in favor of any number of proprietary interfaces. Today’s Ethernet, however, is full duplex, exists on a star topology, and although CSMA/CD is still there, the increased use of 100 Mbps / 1 Gbps transmission and high-speed Ethernet switches to isolate devices into separate collision domains has resulted in a more deterministic type of Ethernet.

Another factor that has discouraged the use of Ethernet in industrial settings is that Ethernet devices were originally developed with PCs in mind. That is, the devices were expected to work well in the same type of environments that PCs are used, such as in the home, in the office, or better yet in the climate controlled corporate machine room. This means that as a rule, “commercial” Ethernet equipment is not reliable enough to work in more demanding industrial settings.

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.

Introducción a Ethernet Industrial



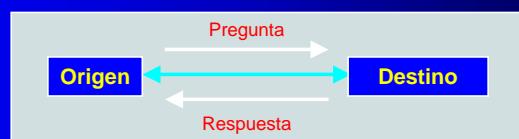
8

Ethernet is a shared media, so there are rules for sending packets of data to avoid conflicts and protect data integrity. Nodes determine when the network is available for sending packets. It is possible that two nodes at different locations attempt to send data at the same time. When both PCs are transferring a packet to the network at the same time, a collision will result.

Minimizing collisions is a crucial element in the design and operation of networks. Increased collisions are often the result of too many users on the network, which results in a lot of contention for network bandwidth. This can slow the performance of the network from the user's point of view. Segmenting the network, where a network is divided into different pieces joined together logically with a bridge or switch, is one way of reducing an overcrowded network.

Comunicación Half Duplex

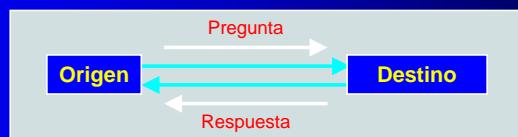
- ❖ Half Duplex: La información puede transmitirse en ambos sentidos, pero no simultáneamente.
- ❖ Una transmisión half duplex usa el mismo canal (físico o lógico) para la comunicación.
- ❖ Un walkie-talkie es un dispositivo half duplex ya que puede hablar solamente una persona a la vez.



Modbus Protocol – Modbus protocol dictates that a sending station must get an answer back from the destination station before the sending station can send a second message to the same destination station. This is a half duplex like communication scheme.

Comunicación Full Duplex

- ❖ 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.



Full duplex operation on a two-wire line requires the ability to separate a receive signal from the reflection of the transmitted signal.

Full duplex requires additional hardware at both the sending and receiving end.

Acceso determinístico Switch Ethernet

- ❖ La tecnología de “Switch” supera esas limitaciones:
 - ❖ Crea dinámicamente redes entre sus puertos, de acuerdo con una tabla interna.
 - ❖ Se crean “dominios de colisiones”, aislados entre si
 - ❖ Cada puerto opera a la máxima velocidad posible, aprovechando el ancho de banda disponible.
 - ❖ Cada dispositivo opera en modo Half DupleX o Full Duplex, sin afectar a los demás.
 - ❖ Logra un alto grado de determinismo en el enlace.

There are means available for working around the determinism problem introduced by CSMA/CD. The first is in the manner that data is transmitted between network devices. Ethernet was originally specified as half-duplex, which meant that a network device could not simultaneously send and receive data. Modern Ethernet, however, is full-duplex, which allows an Ethernet card to begin sending data while still in the process of receiving data (or the other way around). This situation is often characterized by saying that a full-duplex 10 Mbps Ethernet operates at an effective rate of 20 Mbps, since the transmission speed is 10 Mbps each way.

Another way to reduce the chance of data frame collisions is to minimize the number of devices that are connected to the same network. It should be obvious why this has a desirable effect. Fewer devices transmitting data translates into less of a chance that more than one device will attempt to transmit at the same time.

The third remedy to the determinism problem, and the one highlighted in the title of this section, is to use an Ethernet switch to isolate a small number of devices into what is called a “collision domain.” A switch is a specialized junction box that has multiple built-in Ethernet ports and its own processor. Data frames received by the switch are initially forwarded to each of the switch’s ports, but as the switch learns which MAC address is associated with which port, it forwards data frames only to the port associated with the frame’s destination address. As an illustration, consider a network with 500 hosts all contending for use of the same Ethernet. With this number of hosts, there is a good chance that two of the hosts will begin to transmit simultaneously at least some of the time. Suppose now that we use an Ethernet switch to isolate 10 of the network devices into their own “collision domain.” The effect this has is to greatly reduce the chance that messages originating from one of the 10 computers, or intended for one of the 10 computers, will collide. In fact, by putting critical control devices on their own personal collision domain, the chance of collisions is reduced to essentially zero.

Acceso determinístico - Switch Ethernet

❖ Operación:

- ❖ Identifica la dirección de cada uno de los dispositivos conectados a sus puertos en tablas internas.
- ❖ Utiliza un buffer para almacenar y reenviar los paquetes de cada puerto, mediante un bus interno de alta velocidad.
- ❖ Esa información permite establecer redes dinámicas entre cada uno de los puertos.
- ❖ Trabaja a nivel de la capa 2 (Data ó Datalink) del modelo OSI.
- ❖ Utiliza las direcciones de las tarjetas adaptadoras de red (MAC address).

¿Cuándo usar un switch industrial?

- ❖ Aislar la red de planta de la red administrativa.
- ❖ Aislar dispositivos individuales (por su velocidad, por operar en modo half duplex, etc).
- ❖ Proveer un enlace de alta velocidad entre diferentes “dominios” de colisiones.
- ❖ En combinación con conversores de medio a fibra óptica:
 - ❖ Proveer un enlace entre dominios de colisiones alejados entre si.
 - ❖ Brindar alta inmunidad al ruido e interferencias.

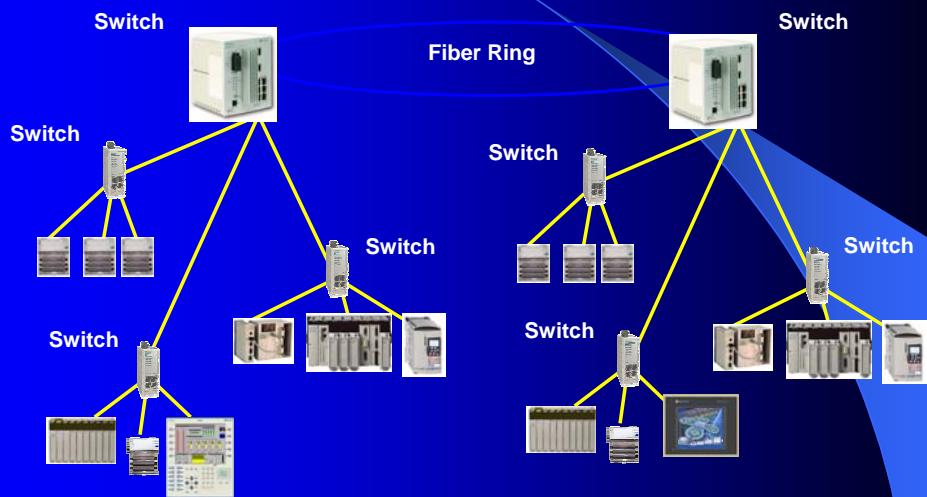
One way to think of Ethernet is as “the great equalizer.” In a very real sense, all devices (this could include PCs, servers, PLCs, sensors, actuators, etc.) that are connected to the same Ethernet LAN are on an equal footing. This is because there is a carefully controlled upper limit to the amount of data that can be sent across an Ethernet with each transmission, and access to an Ethernet is first come first served. Connecting factory computers and devices to a corporate LAN gives engineers ready access to the Internet, and allows the factory and business office to maintain contact via e-mail. It also gives business office and MIS personnel the option to monitor factory floor network activity. The downside to all of this interconnectivity is that data transferred between control devices is easily bogged down by all of the e-mails, MSN activity, and access to various web sites. An Industrial Ethernet Switch can be used to effectively isolate key control devices onto their own collision domain. Engineers can still access the devices from outside the collision domain, but as we pointed out earlier, data transfer within the collision domain is much freer.

This type of application is similar to that described above, but in this case, only one device is connected to each port of the Ethernet switch, essentially isolating the device onto its own collision domain. As a concrete example, control engineers could use one multiport Ethernet switch to connect a PLC to sensor/actuator pairs. Except for the occasional reconfiguration or diagnostic message sent from another part of the network, the switch essentially keeps the control activity completely isolated from the rest of the network.

Some Ethernet switches combine 10 Mbps Ethernet ports with higher speed 100 Mbps ports, with the higher speed ports used to cascade from one switch to another. Two switches of this type can be combined to provide a higher speed connection between separate collision domains. These intra-switch connections are also full-duplex, so that the chance of frame collisions between the two switches is essentially zero.

Some Ethernet switches have both UTP Ethernet ports, which use electrical signals to transmit data, and optical cable ports, which use light pulses to transmit data. Light pulses are immune to interference from lightning and high voltage manufacturing equipment, and in general can be transmitted over a longer distance. This type of Ethernet switch allows to connect one part of a factory floor LAN to another, since the fiber optic cable can be run through areas of the factory that are subject to electromagnetic disturbances, or can be used to go from building to building over distances of several kilometers.

¿Cuándo usar un switch industrial?

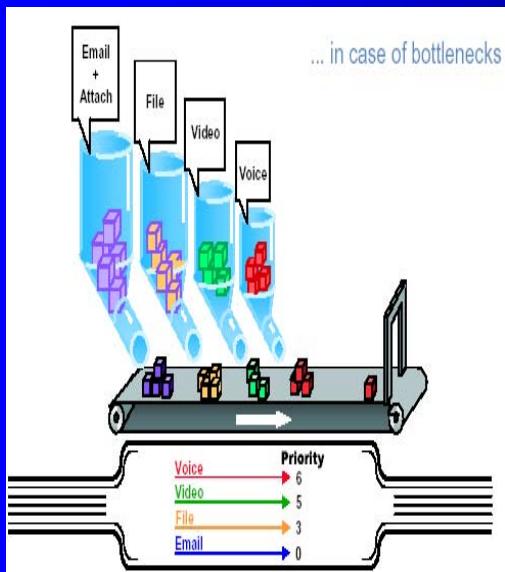


Introducción a Ethernet Industrial

 Telemecanique

14

Prioridad de Mensaje (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.

Introducción a Ethernet Industrial



15

Prioridad de Puerto

- ❖ Permite asignarle 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.

Port	Port Name	Link status	Port on	Flow Control on	Signal Contact mask	Auto-negotiation	Manual Configuration	Current settings	Port Priority
1		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	100 Mbit/s FDX	-	6
2		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	100 Mbit/s FDX	-	5
3		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	100 Mbit/s FDX	100 Mbit/s FDX	0
4		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	100 Mbit/s FDX	100 Mbit/s FDX	0

Port Priority
6
5
0

Introducción a Ethernet Industrial



16

Mayor confiabilidad

- ❖ Alimentación redundante, en diferentes tensiones de CC y CA.
- ❖ Topología en anillo para proveer caminos redundantes de resguardo para la conexión.
- ❖ Diseñados para soportar condiciones extremas de vibración, aceleración y choque.
- ❖ Homologados por organismos reconocidos internacionalmente (IEC, CE, FCC, UL, etc.).
- ❖ Conectores aptos para condiciones extremas de uso.

The above list only gives the basic requirements for industrial applications. When considering industrial communications, reliability means more than just a strong casing and good endurance to extreme temperatures, but also involves more fault resilience functionality. In the office, a 3-minute communication failure could be passed off as a minor inconvenience, whereas in an industrial setting, the same 3 minutes could cause a tremendous loss in investment. With this in mind, the following self-recovery functions can provide the essential functionality needed to keep the network running continuously.

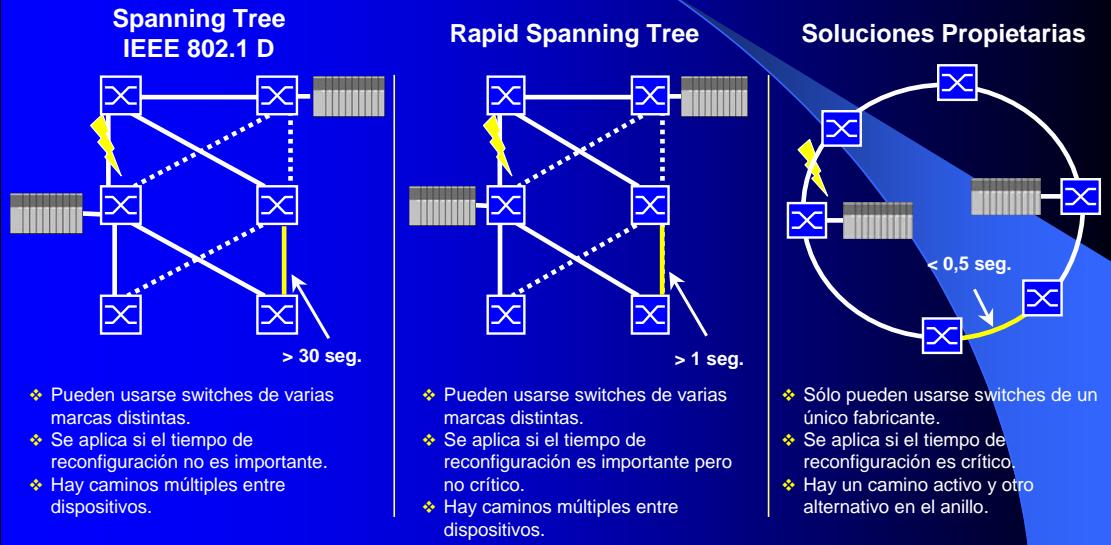
Mayor confiabilidad

- ❖ Componentes electrónicos de grado industrial, para incrementar el MTBF (tiempo medio entre fallas).
- ❖ Rango de temperatura de operación ampliado (40°C a 75°C).
- ❖ Protección contra sobretensiones, hasta 3.000 V.
- ❖ Alimentación de +10 a +30 VCC.
- ❖ Gabinetes herméticos, que reducen el efecto de sustancias nocivas que puedan dañar sus componentes.

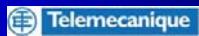
Recuperación rápida

- ❖ Watch-dog y auto-recuperación para prevenir interrupciones aleatorias del servicio.
- ❖ Reconfiguración dinámica de las tablas de enrutamiento para asegurar la comunicación de dispositivos que puedan cambiar de ubicación física, reduciendo el tiempo sin comunicación.

Spanning tree vs. Soluciones Propietarias



Introducción a Ethernet Industrial



20

Spanning Tree

Term for a protocol that is used in ETHERNET networks for path determination. It is specified as Standard IEEE 802.1 D. The spanning tree algorithm prevents the circulation of data packets in a LAN with several possible paths by switching-off individual connections or Ports. In addition it determines the optimum path if there are several alternatives. If a path fails due to the fault or interruption, an alternative connection is searched for using the spanning tree protocol. The reconfiguration of a network of this type may take 30 - 90 seconds.

Spanning-Tree Protocol (STP) prevents loops from being formed when switches or bridges are interconnected via multiple paths. Spanning-Tree Protocol implements the 802.1D IEEE algorithm by exchanging BPDU messages with other switches to detect loops, and then removes the loop by shutting down selected bridge interfaces. This algorithm guarantees that there is one and only one active path between two network devices.

Custom Solutions

Term for a Redundancy process based on the construction of ring-shaped network structures. In rings of these types, network components that supports custom solutions are connected to each other over their backbone or ring ports. A redundancy manager carries out monitoring of the ring and prevents circulating telegrams.

Redundancy manager

Term for a switch or hub in a custom solution, that monitors the ring and in case of an interruption in the ring structure, activates the connection that has been switched-off up to that point. After the interruption has been removed, the redundancy manager again switches this connection off. The ring is thereby physically switched-off, but from the point of view of communication, it is interrupted.

Reportes dinámicos

- ❖ Envío de mensajes (p.e. usando e-mail) al detectar condiciones de excepción, tales como desconexión de dispositivos o saturación de tráfico.
- ❖ Señales discretas de salida para señalizar condiciones de falla en campo.

Since industrial Ethernet devices are often located at the endpoints of a system, such devices cannot always know what's happening elsewhere on the network. This means that industrial Ethernet equipment that connects these devices must take responsibility for providing system maintainers with real-time alarm messages. Even when control engineers are out of the control room for an extended period of time, they can still be informed of the status of devices almost instantaneously when exceptions occur.

The traditional way of determining device status is to poll devices periodically, but this is not real-time enough, and is not very efficient as well. Warning messages must be actively triggered by events. In consideration of these requirements, industrial network equipment must have features such this.

Funciones de administración

- ❖ Verificación de la integridad de la red por medio del comando "ping".
- ❖ Análisis remoto de datos para determinar el comportamiento local de la red desde una ubicación remota.
- ❖ Configuración de "puertos espejo" para una mejor supervisión "en línea" de datos.
- ❖ Asignación de números IP a los dispositivos conectados (DHCP server).
- ❖ Reemplazo de dispositivos dañados.

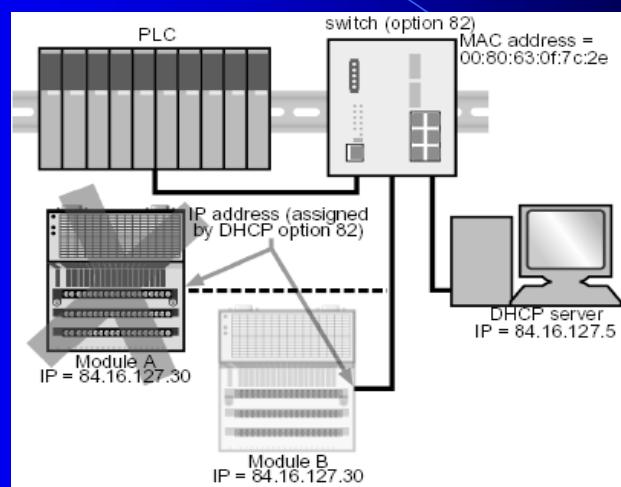
Troubleshooting a network that is experiencing problems can be a real nightmare for maintenance personnel. Quick recovery from network problems is particularly important for industrial applications, since when communication is interrupted, production lines could be halted while waiting for the communication problems to be fixed. The first problem is how maintenance personnel can quickly and effectively find which network segment needs to be fixed. Being able to send "ping" commands that originate from key Ethernet equipment gives network maintainers an essential tool for diagnosing such problems.

The remote data scope utility allows users to easily monitor specific network behavior from a remote networked PC. This utility operates in a manner similar to a regular Data Scope, by allowing users to set a trigger condition, capture port data, and monitor signal status with time stamp. The difference, however, is that instead of monitoring equipment located right next to the Data Scope, users can monitor activity from a remote location, thus giving one maintenance person the ability to monitor many different devices dispersed over a wide area.

Setting up IP addresses is one of the biggest headaches faced by maintenance personnel assigned the task of connecting industrial Ethernet-enabled devices to a network. Unlike PCs, most industrial devices are essentially a "black box," and do not come with a direct human interface. Once the network topology changes or maintenance personnel change, the bothersome process has to be repeated. Making use of Ethernet equipment that can automatically set up your devices' IP addresses can help reduce the effort.

Sometimes a network is just too large, making it difficult to achieve the expected communications behavior. And since Industrial communications applications use more of a command-response style than the file-transfer style used in office network environments, when first setting up an industrial Ethernet network, control engineers may need to use a second port to monitor the actual activity between their devices and computer host. This "mirroring port" helps to ensure that the system behaves as expected.

DHCP Server



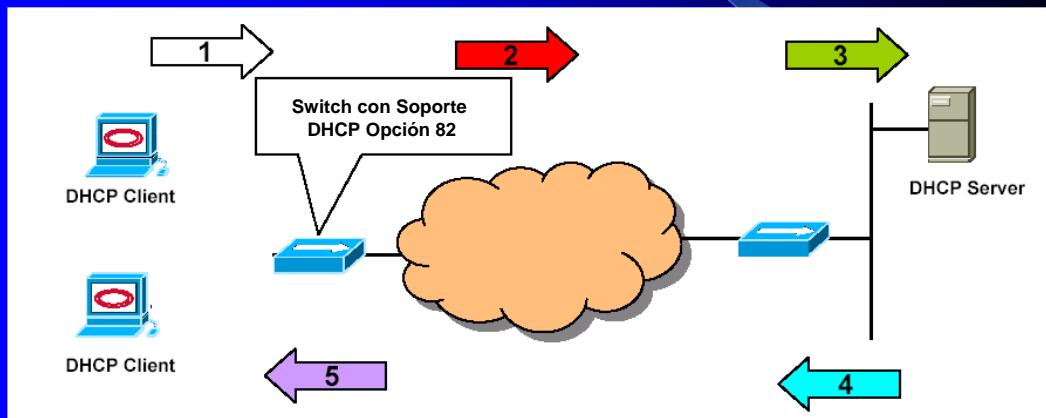
Introducción a Ethernet Industrial



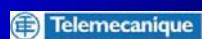
23

Opción 82 DHCP – DHCP Server

1. Pedido DHCP
⇒ Difusión (Broadcast)
2. Opción 82 agrega ID de puerto,
ID de switch e ID de VLAN
⇒ Unicast
3. Servidor DHCP con Opción 82
usa estos parámetros para proveer
la dirección IP



Introducción a Ethernet Industrial



24

Configuración FDR / TFTP

- ❖ La configuración puede almacenarse en un servidor central, corriendo los servicios FDR ó TFTP.
- ❖ La transferencia de la configuración se realiza a partir de la definición del nombre de archivo configurado en el switch:
 - ❖ El nombre de archivo en el servidor FDR lo define el usuario o se basa en el “Role name”.
 - ❖ En el switch se deberá configurar (Telnet serie/Ethernet ó WEB) el nombre de archivo a utilizar.

Funciones de administración

- ❖ Soporte SNMP para simplificar el análisis y la administración de la red.
- ❖ Administración por medio de “OPC Server” para una integración total con los sistemas HMI/SCADA.

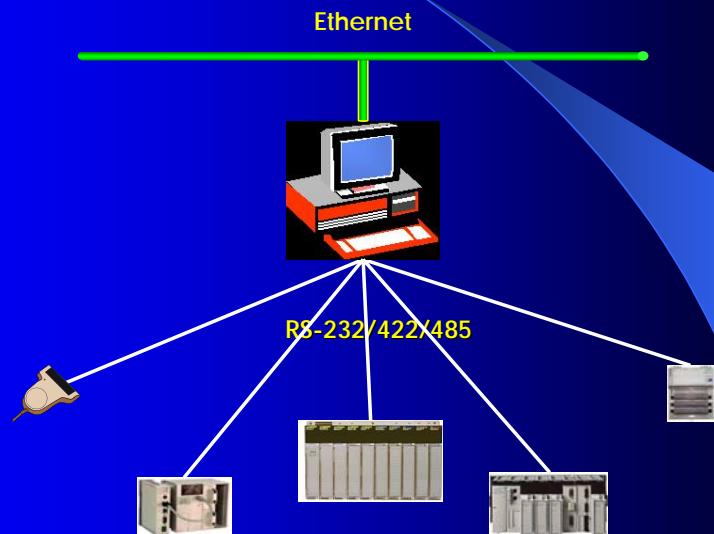
SNMP (Simple Network Management Protocol) is the most popular network analysis protocol used with today's network technology. In fact, it includes many types of well-defined parameters that are available to help you analyze network problems. For example, if too many packets are being broadcast over the network, causing network traffic to build up, it could be due to a device with a bad link, or because of interruptions caused by someone who connects to your network without permission. SNMP gives you the ability to obtain this type of information anytime, and from virtually anywhere.

The OPC specification is a non-proprietary technical specification that defines a set of standard interfaces based on Microsoft's DCOM technology. The application of the OPC standard interface makes possible interoperability between automation/control applications, field systems/devices, and business/office applications. Traditionally, each software or application developer was required to write a custom interface, or server/driver, to exchange data with hardware field devices. OPC eliminates this requirement by defining a common, high performance interface that permits this work to be done once, and then easily reused by HMI, SCADA, Control, and custom applications.

Fácil instalación y mantenimiento

- ❖ Montaje en riel DIN, panel o rack normalizado.
- ❖ LEDs indicadores para verificar el funcionamiento.
- ❖ Conectores para servicio pesado.
- ❖ Soluciones OEM.

Equipos existentes Bridge Serie a Ethernet



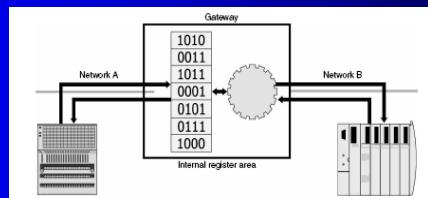
Introducción a Ethernet Industrial

 Telemecanique

28

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.



 Telemecanique

Bridge Serie – Ethernet Memoria Compartida

❖ 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.

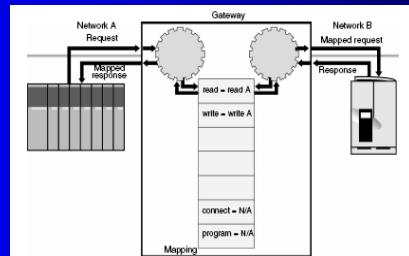
❖ Desventajas:

- ❖ 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).



Telemecanique

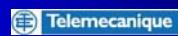
Bridge Serie – Ethernet Conversión de Protocolo

❖ Ventajas:

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

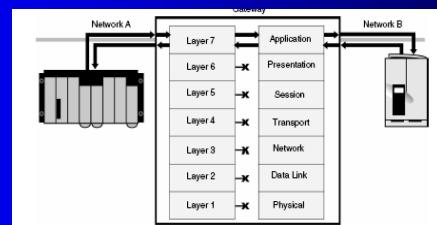
❖ Desventajas:

- ❖ 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.



 Telemecanique

Bridge Serie – Ethernet “Pass Through”

❖ Ventajas:

- ❖ Permite le 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.

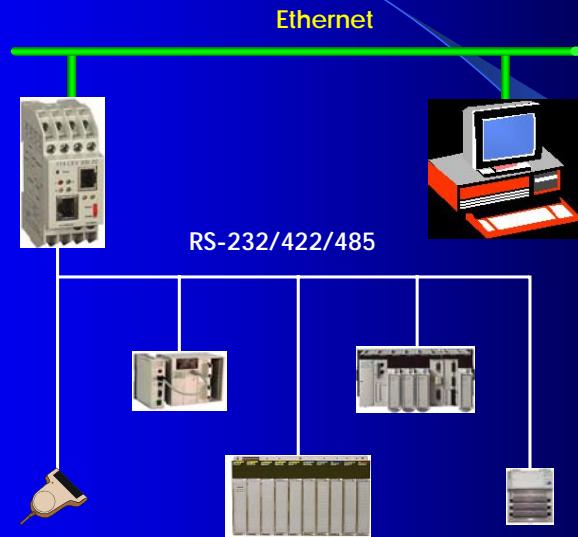


Bridge Serie – Ethernet Conexión Serie Virtual

- ❖ 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.



Bridge Serie – Ethernet Conexión Serie Virtual



Introducción a Ethernet Industrial

 Telemecanique

36

Conexión Serie Virtual

- ❖ Ventajas:

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

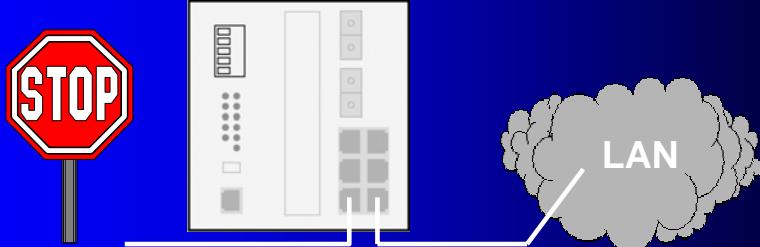
- ❖ Desventajas:

- ❖ 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.



Seguridad de Puerto

- ❖ Por esta funcionalidad cada uno de los puertos del switch puede protegerse para impedir accesos no autorizados.
- ❖ ¿Quién puede acceder a cada puerto?
 - ❖ Todos Sin restricciones de acceso
 - ❖ Ciertos Usuarios Sólo las direcciones físicas (MAC addresses) configuradas
- ❖ ¿Qué sucede cuando hay un intento de acceso no autorizado?
 - ❖ Sin respuesta No hay respuesta
 - ❖ Trap Se envía un mensaje por medio de un "trap" (protocolo SNMP)
 - ❖ Deshabilitar Puerto Se envía un mensaje por medio de un "trap" y se deshabilita el puerto
- ❖ La configuración de seguridad para cada puerto se hace por medio de la administración basada en WEB.



Introducción a Ethernet Industrial

 Telemecanique

38

Seguridad de Puerto

- ❖ Por esta funcionalidad cada uno de los puertos del switch puede protegerse para impedir accesos no autorizados.
- ❖ ¿Quién puede acceder a cada puerto?
 - ❖ Todos Sin restricciones de acceso
 - ❖ Ciertos Usuarios Sólo las direcciones físicas (MAC addresses) configuradas
- ❖ ¿Qué sucede cuando hay un intento de acceso no autorizado?
 - ❖ Sin respuesta No hay respuesta
 - ❖ Trap Se envía un mensaje por medio de un "trap" (protocolo SNMP)
 - ❖ Deshabilitar Puerto Se envía un mensaje por medio de un "trap" y se deshabilita el puerto
- ❖ La configuración de seguridad para cada puerto se hace por medio de la administración basada en WEB.

Port	Allowed MAC address	Current MAC address	Action
1	00 00 00 00 00 00	00 00 00 00 00 00	none
2	00 00 00 00 00 00	00 00 00 00 00 00	none
3	0a 0b 0c 1a 1a bb	00 00 00 00 00 00	none
4	00 00 00 00 00 00	00 0d 56 76 3b 0c	trapOnly
5	00 00 00 00 00 00	00 00 00 00 00 00	none
6	00 00 00 00 00 00	00 00 00 00 00 00	none
7	00 00 00 00 00 00	00 00 00 00 00 00	none
			none
			trapOnly
			portDisable

SNMP Versión 3

- ❖ Prestaciones de Seguridad disponibles en SNMP Versión 3:
 - ❖ Contraseñas encriptadas.
 - ❖ Claves de encriptación basadas en algoritmos robustos, lo que dificulta los “ataques de fuerza bruta”.
 - ❖ Puede encriptarse la información de administración que viaja en la red.

Redes Locales Virtuales VLAN (IEEE 802.1Q)

- ❖ Permite dividir una única red local física en dos o más redes lógicas.
- ❖ Se aísla el tráfico de cada una de las redes virtuales.
- ❖ VLAN basada en los puertos del switch.
- ❖ Los paquetes sin información VLAN (tag) son asignados al puerto correspondiente.
- ❖ Marcado / Desmarcado (Tagging / Untagging):
 - ❖ Las marcas se usan para permitir que varias VLAN comparten el mismo medio físico.
 - ❖ Los paquetes son marcados antes de ser enviados y son reconocidos y direccionaladas a la VLAN respectiva según la marca.
- ❖ La configuración es independiente, la misma dirección MAC puede asignarse a varias VLAN diferentes.
- ❖ Seguridad, se usa un agente de administración separado.

VLANs:

VLANs are based on logical (instead of physical) links and are flexible elements in the network design. The biggest advantage of VLANs is the possibility of forming user groups based on the participant function and not on their physical location or medium.

Since broad/multicast data packets are transmitted exclusively within a virtual LAN, the remaining data network is unaffected.

The VLAN function is defined in the IEEE 802.1Q standard.

Key words often used in association with VLANs are:

Ingress Rule:

The ingress rules stipulate how incoming data is to be handled by the switch.

Egress Rule:

The egress rules stipulate how outgoing data is to be handled by the switch.

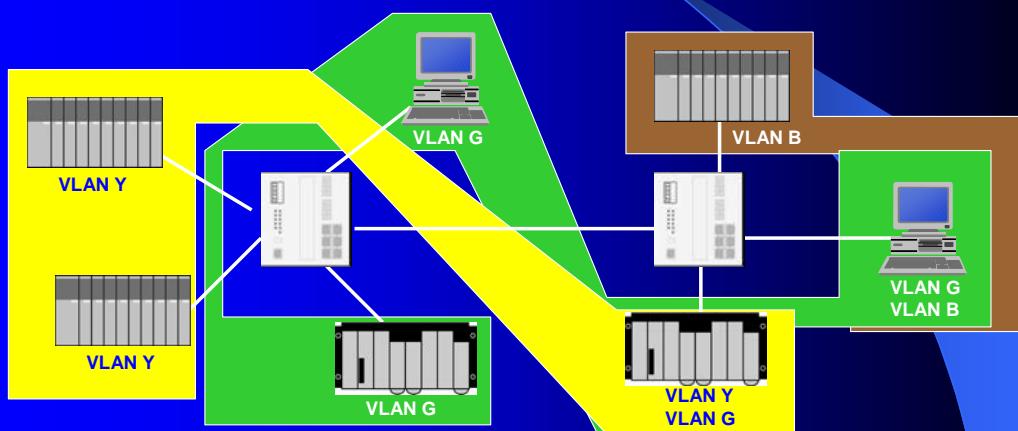
VLAN identifier:

The assignment to a VLAN is effected via a VLAN ID. Every VLAN existing in a network is identified by an ID. This ID must be unique, i.e. every ID may only be assigned once in the network.

Port VLAN identifier (PVID):

The Administration assigns a VLAN ID for every Puerto. It is known, therefore, as the Puerto VLAN ID. The switch adds a tag to every data packet received with no tag. This tag contains a valid VLAN ID. When a data packet is received with a priority tag the switch adds the Port VLAN ID.

Redes Locales Virtuales VLAN (IEEE 802.1Q)

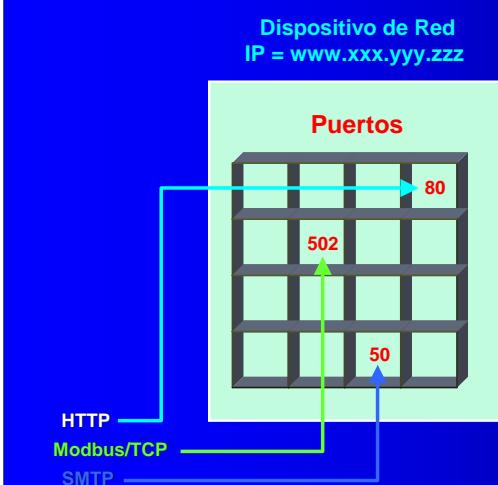


Introducción a Ethernet Industrial



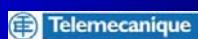
43

Protocolos de Capa de Aplicación Puertos y Sockets



- ❖ Los protocolos TCP y UDP multiplexan las conexiones múltiples a un solo host usando una dirección IP y diferentes números de puertos.
- ❖ Puertos: Cada computadora es dividida en 65.535 puertos:
 - ❖ Los paquetes que ingresan conocen la dirección (IP) y el puerto para los cuales están destinados.
 - ❖ El puerto de destino forma parte del campo de los protocolos TCP y UDP.
- ❖ Los puertos están numerados y son como una casilla de correo:
 - ❖ Un correo para una persona específica sólo es llevado a una sola casilla.
 - ❖ SMTP (Simple Mail Transfer Protocol) va al puerto 50.
 - ❖ HTTP va al puerto 80.
 - ❖ Modbus TCP tiene reservado el puerto 502.
- ❖ Sockets: es la combinación de una dirección IP y un número de puerto; www.xxx.yyy.zzz:nn.

Introducción a Ethernet Industrial

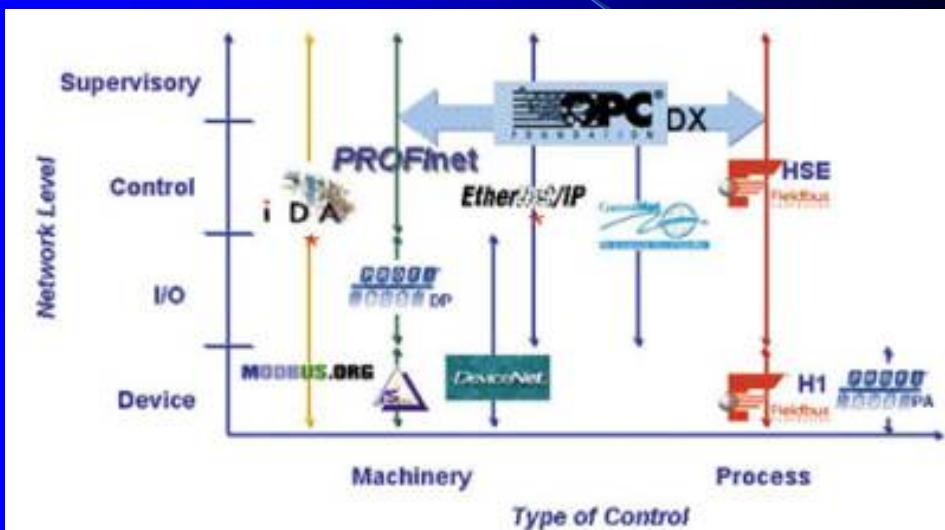


44

A port is analogous to a pigeon hole mail box, where only the mail for any one person is delivered to a hole. With ports, data of a specific type of service is addressed to specific ports, for example Telnet data is directed to port 23, Simple Mail Transfer Protocol (SMTP) is directed to port 25, HTTP to port 80 and Modbus TCP to port 502. A TCP stream is defined by the source and destination IP address and port number, this is for connections between hosts. Internal to the host, this combination of numbers is assigned a unique number called a **socket** and it is the socket that any applications wishing to communicate with other hosts talk to.

When a stream is first initiated, the initiator determines a free port to use as well as which port to talk to on the remote host, for example in an FTP session, the initiator may choose port 1025 to listen on and port 21 to talk to on the remote host (which is the default port for FTP). The listening port is generally determined by the operating system - the user applications have no control over this. When the remote host is sending a packet to the initiator, the same port numbers will be used but their positions in the header will change (source / destination).

Protocolos de Capa de Aplicación



Protocolos de Capa de Aplicación

- ❖ Diferentes buses de campo (fieldbus) utilizan Ethernet como medio físico y para enlace (control de acceso).
- ❖ Estos protocolos representan la implementación a nivel de aplicación (capa 7)
- ❖ Algunas de éstos son:
 - ❖ Modbus/TCP
 - ❖ EthWay
 - ❖ OLE for Process Control Data Exchange (OPC DX)
 - ❖ PROFINet
 - ❖ Interface for Distributed Automation (IDA)
 - ❖ EtherNet/IP
 - ❖ Foundation Fieldbus HSE

Conectividad inalámbrica

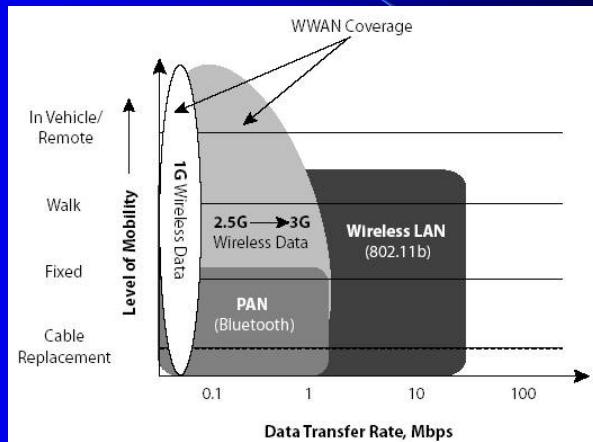


Introducción a Ethernet Industrial

 Telemecanique

47

El espectro y las velocidades



TAKING IT TO THE STREETS: A GUIDE TO WIRELESS FOR THE NON-TECHNICAL BUSINESS PROFESSIONAL. © Intermec Technologies Corp. 2002

El espectro y las velocidades

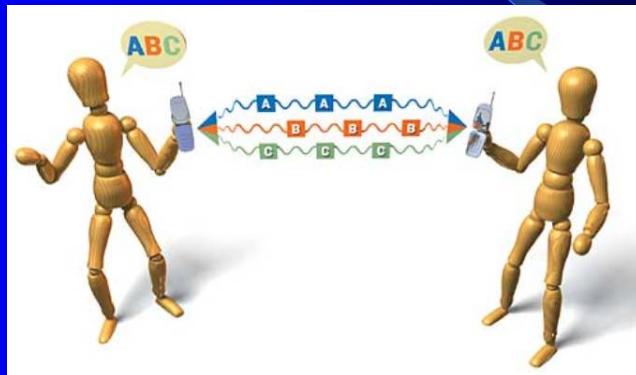


© BRYAN CHRISTIE; IEEE Spectrum March 2004

Introducción a Ethernet Industrial



“Spread Spectrum” en imágenes



© BRYAN CHRISTIE; IEEE Spectrum March 2004

Introducción a Ethernet Industrial



50

Normas IEEE 802.11 ~ Wi-Fi

- ❖ IEEE:

- ❖ The Institute of Electrical and Electronics Engineers.
- ❖ Asociación profesional sin fines de lucro, de alcance mundial, involucrada en tecnologías relacionadas con la computación, las telecomunicaciones, las ingenierías eléctrica, electrónica y biomédica.
- ❖ Importante organismo normalizador.

- ❖ Comité de Normas 802:

- ❖ Se forma en Febrero de 1980
- ❖ Tiene por misión elaborar el cuerpo de normas relativo a la conectividad en red de computadoras y otros dispositivos digitales.
- ❖ El subcomité 802.11 se ocupa de la conectividad inalámbrica, por medio de ondas electromagnéticas, acotada a redes locales.

Conectividad inalámbrica

Normas IEEE 802.11 ~ Wi-Fi

- ❖ 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.)

Características	Normas Wireless LAN		
	802.11b	802.11a	802.11g
Disponibilidad	Muy alta	Tecnología relativamente nueva	Tecnología relativamente nueva, grandes expectativas de crecimiento
Velocidad y Canales por Access Point	1; 2; 5,5 y 11 Mbps 3 canales	6 Mbps; 9 Mbps; 12; 18; 24; 36; 48 y 54 Mbps 8 canales	1; 2; 5,5; 6; 9; 11; 12; 18; 24; 36; 48 y 54 Mbps 3 canales
Costo Relativo	Bajo	Medio alto	Medio
Frecuencia	2,4 GHz (banda no licenciada, usada también por teléfonos inalámbricos, hornos a microondas, etc.)	5 GHz (banda no licenciada, menor probabilidad de interferencias)	2,4 GHz (banda no licenciada, usada también por teléfonos inalámbricos, hornos a microondas, etc.)
Alcance	Hasta 100 metros en interiores (dependiendo del entorno y la velocidad de transmisión)	Hasta 50 metros en interiores (dependiendo del entorno y la velocidad de transmisión)	Hasta 100 metros en interiores (dependiendo del entorno y la velocidad de transmisión)
Acceso Público	Gran disponibilidad de “hotspots” en cyber cafés, aeropuertos, universidades, etc.	No disponible	La interoperabilidad con 802.11b garantiza acceso y favorecerá el cambio en “hotspots” existentes
Compatibilidad	Puede interesar con la 802.11g	Incompatible con 802.11b y 802.11g	Puede interesar con la 802.11b hasta 11 Mbps

Introducción a Ethernet Industrial



52

¿Y la seguridad...?

❖ 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 “Cientes Inalámbricos” y “Access Points”.
- ❖ 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).

Diferentes funciones

- ❖ Router
- ❖ Access Point
- ❖ Bridge Inalámbrico
- ❖ Repetidor
- ❖ Tarjetas adaptadoras (PCI ó PCMCIA)
- ❖ Equipos “Built for Wireless” (p.e. Intel® Centrino™)

Diferentes funciones



Introducción a Ethernet Industrial

 Telemecanique

56

Algunas aplicaciones

- ❖ Logística
- ❖ Sistema de despacho de vehículos
- ❖ Aplicaciones en transporte
- ❖ Control de inventario y recolección de datos en piso de planta
- ❖ Servicios hospitalarios y de salud
- ❖ Puntos de Ventas y de Información móviles (POS/POI)
- ❖ Interfases de operación (HMI) portátiles
- ❖ Telefonía móvil usando “Voice on IP (VoIP)”

Conversores de medio físico

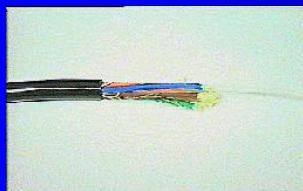


Introducción a Ethernet Industrial



58

Cable de Fibra Optica



- ❖ Consiste de tres partes :
 - ❖ Núcleo (vidrio o plástico).
 - ❖ Cobertura (Cladding).
 - ❖ Vaina de Protección.
- ❖ Núcleo - Provee un canal para el haz de luz.
- ❖ Cobertura - Tubo de vidrio que refleja cualquier rayo de luz hacia el núcleo.
- ❖ Vaina de Protección - Proteje 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 backbone.

Introducción a Ethernet Industrial



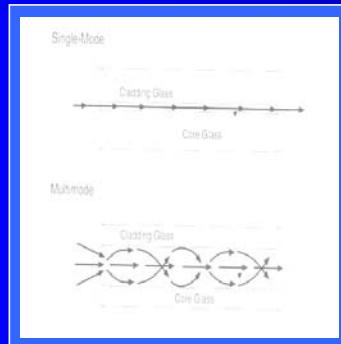
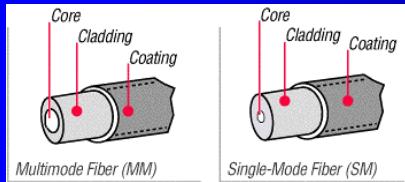
59

Fiber optic cable is considered the default choice for connections involving high speed [large bandwidth requirements like video, large database systems], long distances and interconnecting networks. It costs more than either twisted pair or coax, and requires special connectors and jointing methods.

The features of fiber-optic cable systems are they're expensive, used for backbones [linking LAN's together] or FDDI rings (100 Mbps), high capacity [100 Mbps], immune to electromagnetic interference, low loss, difficult to join, connectors are expensive, the cover long distances.

Fiber optic is often used to overcome distance limitations. It can be used to join two hubs together, which normally could not be connected due to distance limitations. In this instance, a UTP to Fiber transceiver [often referred to as a FOT] is necessary.

Tipos de Fibras Ópticas



- ❖ Mono Modo (Single Mode) - tiene un núcleo mucho más pequeño el cual permite que sólo un haz de luz se propague a través del núcleo.
- ❖ Multimodo (Momo Mode) - tiene un núcleo mucho más grande que la fibra Mono Modo, permitiendo que cientos de rayos de luz se propaguen a través del núcleo simultáneamente.

Introducción a Ethernet Industrial



60

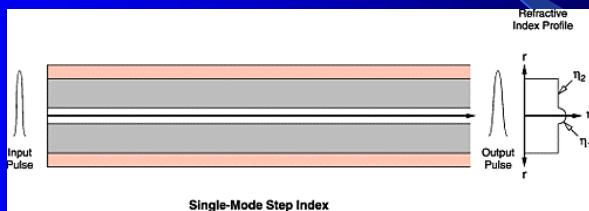
The differences among fibers is their core sizes (the light-carrying region of the fiber). MultiMode cable is made of multiple strands of glass fibers and has a much larger core than Single Mode fiber. MultiMode cables have a combined diameter in the 50-100 um range. (where um is a micron and one micron is 1/250th the width of a human hair). Each fiber in a MultiMode cable is capable of carrying a different signal independent from those on the other fibers in the cable bundle. These larger core sizes generally have greater bandwidth and are easier to couple and interconnect. It allows hundreds of rays to light to propagate through the fiber simultaneously. MultiMode fiber today is used primarily in premise applications, where transmission distances are less than two kilometers.

Single Mode fiber is a single strand of glass that has a much smaller core that allows only one mode of light to propagate through the core. Single Mode fiber has a higher bandwidth than MultiMode and for this reason it is the ideal transmission medium for many applications. The standard Single Mode fiber core is approximately 8-10 um in diameter. Because of its greater information-carrying capacity, Single Mode fiber is typically used for longer distances and higher-bandwidth applications.

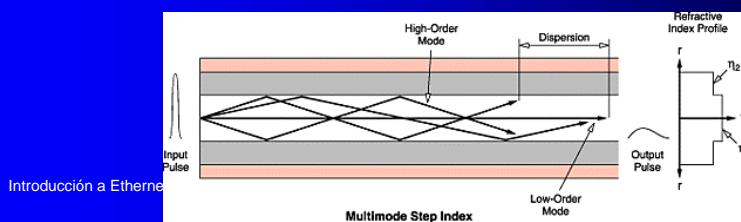
While it might appear that MultiMode fibers have higher information carrying capacity, this is not the case. Single Mode fibers retain the integrity of each light pulse over longer distances which allows more information to be transmitted. This is why MultiMode fibers are used for shorter distances.

Cable de Fibra Optica: Mono y Multimodo

- ❖ La fibra Mono modo tiene mejor desempeño, cubre mayores distancias y es una tecnología más cara que la fibra multimodo.



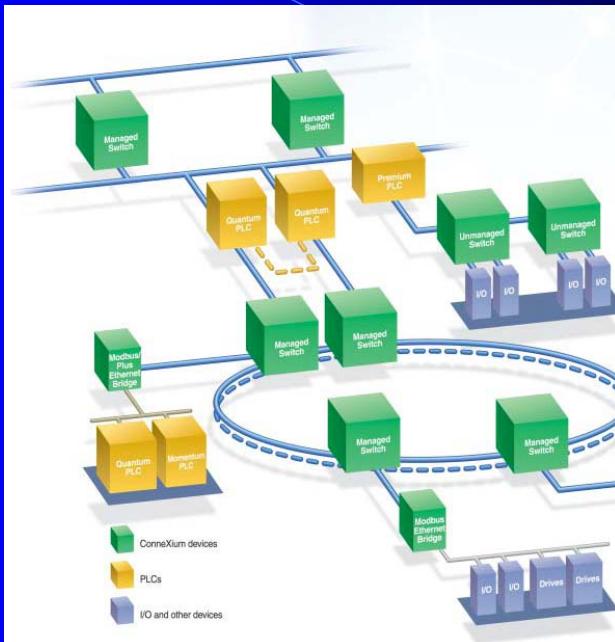
- ❖ La fibra Multi modo está limitada a longitudes de uno o dos kilómetros, dependiendo de la aplicación.



61

Introducción a Ethernet

Resumiendo



Introducción a Ethernet Industrial

Telemecanique

62

Referencias

- ❖ <http://www.ieee.org/>
- ❖ <http://standards.ieee.org/wireless/index.html>
- ❖ <http://www.aadeca.org/>
- ❖ <http://www.iec.ch/>
- ❖ <http://www.modbus.org>
- ❖ <http://www.modbus-ida.org/>
- ❖ <http://www.opcfoundation.org/>
- ❖ <http://www.fieldbus.org/>
- ❖ <http://www.profibus.com/>
- ❖ <http://www.ethernet-ip.org/>
- ❖ <http://www.iaona.org/>
- ❖ <http://ethernet.industrial-networking.com/>
- ❖ <http://www.tropsoft.com/strongenc/des.htm>
- ❖ <http://www.weca.net/>
- ❖ <http://www.bitpipe.com>
- ❖ <http://www.plcopen.org>
- ❖ <http://www.automation.com>
- ❖ <http://www.plcs.net>
- ❖ <http://www.automatas.org/>
- ❖ <http://www.ccontrols.com/>

Introducción a Ethernet Industrial



63

¡Muchas gracias...!

diego.romero@ar.schneider-electric.com

