Transmisión de datos industriales
Aplicaciones teóricas y generales

WESTERMO

Manual
Westermo
5.0

Primera edición publicada en diciembre de 1994. © Westermo, Suecia, 1994.
Segunda edición publicada en 1996. © Westermo, Suecia, 1996.
Edición 2.1 publicada en 1997. © Westermo, Suecia, 1997.
Edición 3.0 publicada en 1998. © Westermo, Suecia, 1998.
Edición 4.0 publicada en 2001. © Westermo, Suecia, 2001.
Edición 5.0 publicada en 2004. © Westermo, Suecia, 2005.
Redacción: Westermo Teleindustri AB, Suecia.
Ilustraciones: Visual Information Sweden AB, Eskilstuna.
Fotografía: bildN, Västerås, Suecia.
Björn Fröberg, Jordnära bildform, Eskilstuna, Suecia
futureimagebank.com
Repro: Ågerups Repro AB, Eskilstuna, Suecia.
Impresión: Eskilstuna Offset AB, Eskilstuna, Suecia.

Estimado lector:

Tiene entre sus manos la quinta edición del manual Westermo. La primera edición del manual se publicó hace ya diez años, en 1994, y con el tiempo se ha convertido en una herramienta que utilizan tanto los ingenieros como todas aquellas personas interesadas en la transmisión de datos.

Al igual que en las ediciones anteriores, nuestro objetivo es ofrecer una presentación pormenorizada de la gama de productos Westermo, pero acompañándola de una completa descripción de los aspectos teóricos básicos de la transmisión de datos. Las secciones dedicadas a las aplicaciones teóricas y generales han ido aumentando con cada nueva edición del manual, y esta quinta no es una excepción.

Con todo, esta edición del manual presenta diferencias con respecto a las anteriores. En efecto, el significativo aumento de nuestra gama de productos nos ha obligado a dividir el manual en secciones más manejables.

Como resultado, encontrará en el manual las secciones siguientes:

- Aplicaciones teóricas y generales
- Conexión remota
- Ethernet industrial
- Transmisión local de datos

Esperamos que el manual Westermo se convierta en una herramienta útil que le ayude en su trabajo diario y que venga a completar la asistencia y el soporte que presta nuestro personal dedicado repartido por todo el mundo.

Índice

Transmisión de datos – algo más que cables y conectores 10–13
Transmisión de datos industriales 10
La revolución de la TI industrial 10
Diferentes normas 10
Transmisión de datos industriales 10
¿Qué significa para nosotros la transmisión de datos industriales? 11–13
Eliminación de los tiempos de inactividad 11
Eliminación del mantenimiento 11
Entornos adversos 11
Rango de temperaturas ampliado 11
Comportamiento mecánico 11
Aislamiento galvánico 12
Eliminación de los transitorios 12
Alimentación 12
Determinismo 13
Homologaciones 13
Datos técnicos generales 14–23
Condiciones ambientales y mecánicas 14
Entorno industrial 14
Instalación en exteriores 14
Condiciones eléctricas 15
1.1 Emisiones generales 16
1.2 Emisiones de los equipos de tecnología de la información 16
1.3 Inmunidad de los equipos de tecnología de la información 16
1.4 Inmunidad general 17
1.5 Método de ensayo de la compatibilidad electromagnética 17
Niveles de severidad CEM en diferentes entornos 18
Residencial 18–20
Aplicaciones ferroviarias 18–20
Subestaciones 18–20
Westermo 18–20
Condiciones de seguridad 21
Condiciones de instalación 21
1.6 Seguridad eléctrica 22
Caja 22
1.7 Grado de protección 22
1.8 Inflamabilidad 23
2 Definiciones 23
2.1 Rango de tensiones nominales 23
2.2 Rango de tensiones de funcionamiento 23
2.3 SELV 23
2.4 TNV-1 23
2.5 TNV-3 23

La transmisión de datos es imprescindible para aumentar la productividad 24–55
Interfaz 24
Interfaces más comunes 24–25
Señales de V.24/RS-232-C 25
Configuración de cable 26
Clave de las señales más importantes 27
ASCII 28
Interfaces industriales 29-30
RS-422 29
RS-422 a 4 hilos 29
RS-485 29
Terminación y sistema a prueba de fallos 30
Polaridad 30
Convertidor RS-232/V.24 a RS-422/485 – Soporte de RTS 30
Instalación de RS-422 y RS-485 31–32
Recomendaciones generales de instalación 31
Distancia de transmisión y módems de corto alcance 31
Bucle de corriente de 20 mA (TTY) 31
Bucle de corriente simétrica de 10 mA (W1) 32
Por tanto, el bucle de corriente de 10 mA es menos sensible a las fuentes de interferencias externas 32
Red 33–34
Topología 35–36
Red punto a punto serie 35
Red en estrella 35
Red en anillo 35
Red de bus 36
Red mixta 36
Red en malla 36
El problema de las interferencias 37–42
Rayos, maquinaria y tubos fluorescentes 37–38
Protección contra rayos y sobretensiones 38–39
Bucles de tierra 39
Reducción de las interferencias 40
Señales simétricas 40
Aislamiento 40
Redes a tierra 41
Apantallamiento 41
Conexiones a corta distancia sin módem 41
Módems telefónicos e interferencias 42
Cable de fibra óptica 42

Tipos de cables de cobre 43–44
Par trenzado 43
Cable coaxial 44
Distancia y diseño 44–55
Distancias de transmisión con diferentes tipos de cable y velocidades 44
Cálculo de la resistencia 45
Dos maneras de expresar la capacidad 45
Marcado de los cables 46
Transmisión de datos por fibra óptica 47
Cable de fibra óptica 47
Material 48
Atenuación en la fibra multimodo 48
Multimodo 48
Atenuación en la fibra monomodo 49
Longitud de onda 49
Atenuación de la luz en cable de fibra de vidrio a diferentes longitudes de onda 50
Terminación 51
Cálculo del balance de pérdida 52
Ejemplo 52
Modelo OSI 53
Estructura del modelo OSI 53
Ejemplo comparativo 54–55
Transmisión local de datos 56–65
Buses de campo 56–57
Buses de campo 57
PROFIBUS 58
Historia 58
Comunicación PROFIBUS 58
Topología de red de PROFIBUS 59
PROFIBUS DP 60
Modbus 61
Modbus Plus 62
Modbus/TCP 62
LON®WORKS 63–65
Consideraciones sobre las redes LonTalk® grandes 65
Conexiones remotas 66–109
Líneas conmutadas PSTN 66
Transmisión de datos por la red de telefonía fija 66
Conexión por línea conmutada 66
Modulación 67
¿Es lo mismo un bit por segundo que un baudio? 68
Algunas normas 69
V.90 69

Conexión ... 70
Lenguaje de los módems telefónicos ... 70
Corrección de errores y compresión ... 70
Búsqueda y transferencia de archivos ... 70
Las autopistas del futuro ... 71
Líneas dedicadas ... 71
V.23 sobre línea dedicada ... 72
Módem V.23 de Westermo ... 72
Uso de HyperTerminal (R) ... 73–80
TDtool ... 76–77
Comandos AT ... 78–80
Mayor velocidad ... 81–83
xDSL ... 81
HDSL ... 81
ADSL ... 81
VDSL ... 81
SDSL ... 82
SHDSL ... 82
G.703 ... 83
GSM ... 84–96
Historia de la tecnología GSM ... 84–85
Arquitectura ... 85
Componentes de la red ... 86
Estructuras celulares ... 87
Transmisiones de radio entre MS y BSS ... 87–88
Servicios de la red GSM ... 89-92
Telefonía ... 89
Servicio de transmisión de datos con conmutación de circuitos ... 89
SMS ... 90
MMS ... 90
Fax ... 90
GPRS ... 91–92
Seguridad de las redes ... 92–95
GSM ... 92
GPRS ... 92
Diferencias entre GSM y GPRS ... 93
Aplicaciones con GSM y GPRS ... 93–95
Clases de GPRS ... 96
UMTS (3G) ... 96
RDSI ... 97–104
¿Qué es RDSI? ... 97
Señalización ... 97
Conexiones ... 97

Interfaz/componentes de las líneas RDSI ... 98
Capa física ... 99
Formato de trama en la interfaz S ... 100
Capa 2 – Capa de enlaces de datos ... 101
SAPI ... 102
TEI ... 102
Capa 3 – Capa de red ... 103
CAPI ... 104
Radio ... 105–109
Radiocomunicaciones ... 105
Funcionamiento de la comunicación por radio ... 105
Atenuación y ruido ... 106
Antenas ... 107–109
Terminología ... 107
La antena y sus componentes ... 107
Tipos de antenas ... 108
Propagación de la señal ... 108
Red radioeléctrica ... 109
Ethernet industrial ... 110–145
IEEE 802.3 Ethernet ... 110
Métodos de acceso ... 110
Direcciones y paquetes en Ethernet ... 111
Dominio de colisiones ... 112–113
Redes IP ... 113–122
Protocolo de Internet (IP) ... 113
Métodos de direccionamiento ... 113
Direcciones de red ... 114
Direcciones públicas y privadas ... 115
Ipv4 e Ipv6 ... 116
División de la subred ... 116–117
Puertos ... 118
ARP ... 118
Punto a Punto (PPP) ... 119
Seguridad (CHAP y PAP) ... 119–120
CHAP es un protocolo mucho más seguro que PAP ... 120
TCP/IP y UDP/IP ... 121
UDP ... 121
TCP ... 121
Cómo se establece la conexión TCP ... 122
Cómo construir una red ... 123–126
Dispositivos de la red ... 123–126
Repetidores ... 123
Bridge ... 123

Router 124–125
Brouter 125
Hub 125
Switch 126
Gateway 126
Firewall 126
Hub o switch 127
Diferentes tipos de switches 128
FRNT y el protocolo de árbol de extensión (Spanning Tree) 128
Switch para red en anillo 129
FRNT0 129
FRNT1 129
Switches con servidor de tiempo 130
Funciones del switch 131–132
Priorización (QoS, **Q**uality **of S**ervice) 131
Prioridad de capa 2 131
Prioridad de capa 3 132
Prevención HOL (Head of Line) 133–143
VLAN 134
IGMP/IGMP snooping 135
Redes con sincronización horaria 136
SNTP/NTP 137
Inserción de marcas horarias mediante aplicaciones 137
Inserción de marcas horarias mediante controladores Ethernet 137
Inserción de marcas horarias en la capa física 137
SNMP 138
Software SNMP 139
SNMP, SNMPv2 y SNMPv3 140
MIB 141
OPC 141–143
Ethernet por cable 144–145
Ethernet de 10 Mbit/s 144–145
Fast Ethernet 144–145
Gigabit Ethernet 144–145
Glosario 146–158

Transmisión de datos – algo más que cables y conectores

Transmisión de datos industriales

La revolución de la TI industrial

La implantación de canales de información nuevos y eficaces en los procesos de las empresas puede proporcionar grandes ventajas competitivas. Algunos conceptos clave hoy día, tales como el desarrollo de productos más rápidos, la producción orientada al cliente o los tiempos de conversión y de distribución más cortos, son el resultado de la introducción de las tecnologías de la información en el sector industrial, como también lo son el acceso rápido a la información o la posibilidad de controlar los procesos. La industria desarrolla herramientas de TI que requieren mayor integración en todas las etapas del proceso, desde las compras y la producción, hasta la comercialización. En la actualidad, la calidad de los flujos de información y de las vías por las que éstos discurren es una de las condiciones más importantes para mejorar la eficacia y la competitividad en el sector industrial.

Diferentes normas

Cada día surgen nuevas ideas, nuevos sistemas y nuevas soluciones para desarrollar estas herramientas. Sin embargo, toda esta dinámica y diversidad ha tenido una consecuencia negativa: durante mucho tiempo, y a pesar de los numerosos intentos, ha sido imposible disponer de normas aceptadas, pues cada desarrollador creaba su propia solución. El problema de la falta de normalización surge cuando se hace necesario conectar ordenadores, máquinas y equipos de forma que se comuniquen entre sí, y afecta a todos los niveles, no sólo a los cables y conectores. Afecta a la manera en que se crean, guardan, comprimen, direccionan y envían los datos; a la manera en que el medio (por ejemplo, un cable) transporta, recibe y descomprime la información, y a la manera en que el receptor la lee. Sólo cuando todo esto funciona se consigue establecer una transmisión de datos eficaz. Sólo cuando todas las piezas encajan se cumple la condición indispensable para el desarrollo de las tecnologías de la información en el sector industrial.

Transmisión de datos industriales

Los avances más importantes en la normalización de la transmisión de datos han tenido lugar en las oficinas, con sus redes integradas de ordenadores personales, mainframes, impresoras, servidores, módems telefónicos, etc. En cambio, la transmisión local de datos en las aplicaciones industriales ha resultado más problemática, debido a la inexistencia de normas aceptadas y a que la diversidad es aún mayor cuando la comunicación es entre equipos tan distintos como, por ejemplo, ordenadores, tornos, instrumentos de medición, básculas, autómatas, sistemas de transporte y diferentes sistemas de alarma. Además, los requisitos de fiabilidad e inmunidad a las interferencias son mayores en la industria. Estos son los motivos que nos han llevado a escribir este manual, para aclarar conceptos, explicar cómo funciona la transmisión de datos industriales y proporcionar una guía práctica que ayude a resolver los problemas que conlleva. Si desea más información, no dude en ponerse en contacto con Westermo.

¿Qué significa para nosotros la transmisión de datos industriales?

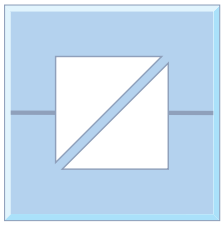
Eliminación de los tiempos de inactividad
Todos los equipos deben estar diseñados de manera que no haya interferencias en la transmisión ni tiempos de inactividad. Para lograrlo, en Westermo utilizamos componentes de la máxima calidad, tales como condensadores de larga vida útil, y validamos los diseños en entornos expuestos a interferencias.

Eliminación del mantenimiento
Nuestros productos están diseñados para resistir los entornos más adversos, sin necesidad de mantenimiento. Además de su robusto diseño, nuestros productos nunca contienen componentes que haya que sustituir, como baterías.

Entornos adversos
Los equipos de TI para entornos industriales se suelen instalar junto a máquinas que generan interferencias, como equipos de soldadura o maquinaria pesada. En Westermo aprovechamos al máximo la experiencia acumulada a lo largo de más de 30 años para diseñar equipos de transmisión de datos capaces de trabajar en los entornos más adversos.

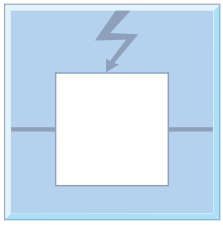
Rango de temperaturas ampliado
Las aplicaciones industriales suelen requerir un rango de temperaturas ampliado. Para garantizar la funcionalidad, en Westermo utilizamos siempre hardware (por ejemplo, conectores) de elevada calidad y capaz de trabajar a temperaturas más extremas.

Comportamiento mecánico
En las aplicaciones industriales, los equipos de TI se suelen instalar en máquinas que se mueven o vibran. Por eso todos nuestros productos están diseñados para soportar tensiones mecánicas elevadas. Como además el método de montaje es tan importante como la fiabilidad mecánica, nuestra gama incluye productos para bastidor y montaje DIN, así como modelos de sobremesa y minimódems.



Aislamiento galvánico

Entre las causas más frecuentes de los errores en la transmisión de datos se encuentra la diferencia de potencial entre los equipos interconectados. La mejor manera de eliminar el problema es garantizar el aislamiento galvánico entre las interfaces, una de las características básicas de nuestros productos.



Eliminación de los transitorios

Los equipos de TI para entornos industriales suelen estar expuestos a diferentes formas de transitorios y a interferencias generadas por cables de alta tensión, cargas reactivas, etc. Westermo elimina el problema desarrollando productos capaces de resistir este tipo de perturbaciones.

Alimentación

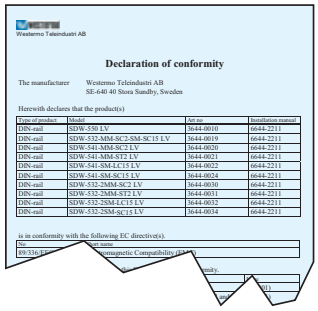
Para eliminar los tiempos de inactividad, los equipos de TI industriales requieren una fuente de alimentación fiable, por lo que a menudo se utiliza una fuente de corriente continua con baterías de respaldo. Sin embargo, como la tensión de recarga de las baterías es más alta que la nominal, todos los equipos deben haber sido diseñados teniendo en cuenta esta circunstancia. A veces también es importante utilizar una fuente de alimentación redundante para aumentar la fiabilidad. Muchos de nuestros productos utilizan este sistema.

Determinismo

Cuando se utilizan equipos en aplicaciones en tiempo real es importante poder definir niveles de prioridad. Nuestros switches incorporan funciones y colas que garantizan la transmisión de datos priorizados.

Homologaciones

Tener instalados productos en aplicaciones de muy diverso tipo de todo el mundo obliga a cumplir las normas de seguridad y los requisitos locales de inmunidad eléctrica/ emisiones y mecánicos. Para ello, en Westermo diseñamos y fabricamos todos nuestros productos con arreglo a las normas internacionales.



Westermo Teleindustri AB

Declaration of conformity

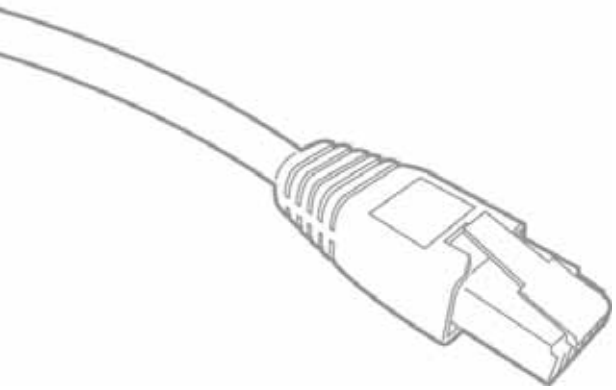
The manufacturer Westermo Teleindustri AB
SE-640 40 Stora Sandby, Sweden

Herewith declares that the product(s)

Type of product	Model	Art.no	Installation manual
DIN-rail	SDW-550 LV	3644-0010	6644-2211
DIN-rail	SDW-532-MM-SC2-SM-SC15 LV	3644-0019	6644-2211
DIN-rail	SDW-541-MM-SC2 LV	3644-0020	6644-2211
DIN-rail	SDW-541-MM-ST2 LV	3644-0021	6644-2211
DIN-rail	SDW-541-SM-LC15 LV	3644-0022	6644-2211
DIN-rail	SDW-541-SM-SC15 LV	3644-0024	6644-2211
DIN-rail	SDW-532-2MM-SC2 LV	3644-0030	6644-2211
DIN-rail	SDW-532-2MM-ST2 LV	3644-0031	6644-2211
DIN-rail	SDW-532-2SM-LC15 LV	3644-0032	6644-2211
DIN-rail	SDW-532-2SM-SC15 LV	3644-0034	6644-2211

is in conformity with the following EC directive(s).

No.	EC name
89/336/EEC	Electromagnetic Compatibility (EMC)



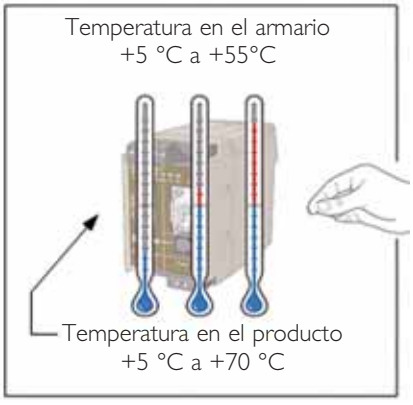
Datos técnicos generales

Condiciones ambientales y mecánicas

	Requisito		
Factor	**Severidad**	**Norma**	**Comentarios**
Temperatura de funcionamiento	+5 a +55 °C –25 a +70 °C*	IEC 721-3-3	
Temperatura de almacenamiento y transporte	–25 a +70 °C	IEC 721-3-1/2	
Humedad relativa de funcionamiento	5 a 95%, sin condensación	IEC 721-3-3	No utilizar hasta que la temperatura y la humedad sean estables
Humedad relativa de almacenamiento y transporte	5 a 95%, condensación permitida en el exterior del embalaje	IEC 721-3-1/2	Producto embalado
Contaminantes atmosféricos Nivel de severidad	G2 (1000 Å=0,1 µm) Moderado	ISA 71.04	Producto instalado en caja IP 21 o superior, con circulación de aire limitada (sin ventilador)

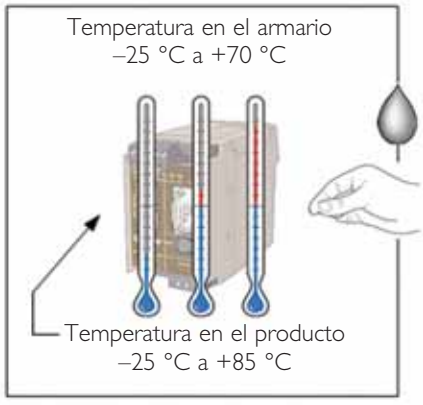
* Rango de temperaturas ampliado

Entornos industriales
Temperatura de funcionamiento admisible: +5 °C a +40 °C



IP20
- Protección contra el acceso a partes en tensión
- Protección contra la penetración de cuerpos sólidos extraños de diámetro ≥12,5 mm

Instalaciones en exteriores
Temperatura de funcionamiento admisible:
–25 °C a +55 °C



IP21
- Protección contra el acceso a partes en tensión
- Protección contra la penetración de cuerpos sólidos extraños de diámetro ≥12,5 mm
- Protección contra la penetración de agua por caída vertical de gotas de agua

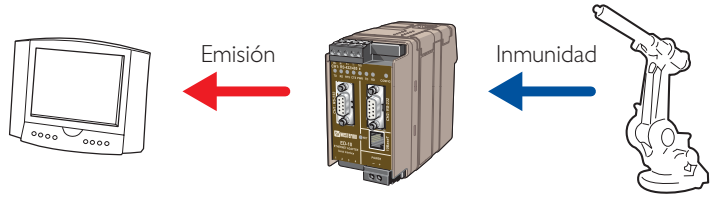
Las especificaciones existentes sobre rangos de temperatura y clasificación IP abarcan distintos niveles. Nosotros diferenciamos entre los entornos industriales y las instalaciones en exteriores. Los componentes diseñados para las distintas variantes deben ser capaces de soportar la temperatura ambiente y también el calor que se genera en las cajas y armarios. En términos generales, se considera que cada caja produce un aumento de temperatura de 15 °C, lo que significa que, para poder garantizar el funcionamiento a una temperatura ambiente (fuera del armario) de +55 °C, tenemos que seleccionar componentes adecuados para temperaturas de +85 °C.

Condiciones eléctricas

	Requisito			
Factor	**Severidad**	**Norma**	**Comentarios**	**Referencia**
Emisión	EN 61000-6-3 Residencial	EN 55022 clase B		**Apartados 1.1 y 1.2**
Inmunidad	EN 61000-6-2 Industrial	EN 61000-4-2 EN 61000-4-3 EN 61000-4-4 EN 61000-4-5 EN 61000-4-6 EN 61000-4-8 EN 61000-4-11		**Apartados 1.1 y 1.2**
	Equipos de tecnologías de la información	EN 55024		**Apartado 1.3**
Alimentación (BT) Rango de tensiones nominales	12 a 48 VCC			**Apartado 2.1**
Rango de tensiones de alimentación	9,6 a 57,6 VCC			
Alimentación (AT) Rango de tensiones nominales	95-240 VCA 110–250 VCC			**Apartado 2,2**
Rango de tensiones de alimentación	85,5–264 VCA 88–300 VCC			
Rango de frecuencias de alimentación nominales	48 – 62 Hz			
Protección contra la inversión de polaridad	Sí			
Protección contra cortocircuitos	Integrada en la instalación del edificio			
TNV-3	Máximo pico de 70,7 V / 120 VCC		PSTN o similar	**Apartado 2.5**
TNV-1	Máximo pico de 42,4 V / 60 VCC		RS-422/485, Ethernet o similar	**Apartado 2.4**
SELV	Máximo pico de 42,4 V / 60 VCC		RS-232 o similar	**Apartado 2.3**

1.1 Emisiones generales

EN 61000-6-3 CEM – Normas genéricas – Norma de emisión en entornos residenciales, comerciales y de industria ligera.



Inmunidad = Tolerancia a las perturbaciones del entorno.
Emisión = Influencia en el entorno (energía emitida).

El nivel de emisión de nuestros equipos es aproximadamente 100.000 veces más bajo que su nivel de inmunidad.

Establece los niveles máximos de interferencias de radio generadas por el equipo conectado a la red pública o a una fuente de alimentación CC. Los requisitos relativos a los niveles de emisión se determinan de manera que las interferencias generadas por el equipo durante el funcionamiento normal en hogares, oficinas, comercios y entornos similares no superen un nivel tal que obstaculice el funcionamiento adecuado de otros equipos (como receptores de radio, por ejemplo).

1.2 Emisiones de los equipos de tecnología de la información

EN 55022 Equipos de tecnología de la información – Características de perturbación radioeléctrica – Límites y métodos de medición.

- Establece métodos de medición y valores límite de las interferencias de radio generadas por los equipos de tecnología de la información.
- Clase B: equipo de tecnología de la información diseñado para hogares, oficinas, comercios y entornos similares. No garantiza la protección contra las interferencias de radio y TV cuando se utiliza a menos de 10 m de la antena receptora.
- Clase A: equipo de tecnología de la información diseñado para el resto de entornos (entre ellos el industrial). No garantiza la protección contra las interferencias de radio y TV cuando se utiliza a menos de 30 m de la antena receptora.

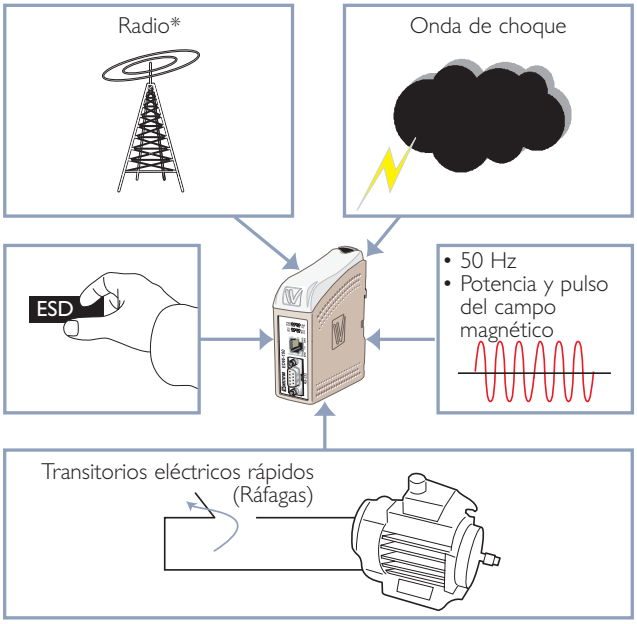
1.3 Inmunidad de los equipos de tecnología de la información

EN 55024 Equipos de tecnología de la información – Características de inmunidad – Límites y métodos de medición.

- Establece ensayos de inmunidad de los equipos de tecnología de la información a las perturbaciones continuas y transitorias, radiadas y conducidas, incluidas las descargas electrostáticas. Los requisitos de inmunidad garantizan un nivel satisfactorio de inmunidad inherente, para que el equipo funcione adecuadamente en el entorno en el que se encuentre.

1.4 Inmunidad general

EN 61000-6-2 Compatibilidad electromagnética (CEM). Normas genéricas. Norma relativa a la inmunidad en entornos industriales.



* Inmunidad a los campos radiados.
Campos de radio-frecuencia conducidos.

Establece ensayos de inmunidad de los equipos conectados a redes en entornos industriales a las perturbaciones continuas y transitorias, radiadas y conducidas, incluidas las descargas electrostáticas. Los requisitos de inmunidad garantizan un nivel satisfactorio de inmunidad de los equipos en los entornos industriales.

1.5 Método de ensayo de la compatibilidad electromagnética (CEM)

EN 61000-4-2 Compatibilidad electromagnética (CEM). Técnicas de ensayo y medición. Ensayo de inmunidad a las descargas electrostáticas.

- Método de ensayo de la inmunidad del equipamiento eléctrico a las descargas electrostáticas provocadas directamente por las personas o por objetos adyacentes. Establece varios niveles de ensayo que se corresponden con diferentes condiciones de instalación y entorno.

Niveles de severidad CEM en diferentes entornos

Residencial
Entornos residenciales, comerciales y de industria ligera.

Industrial
Inmunidad en entornos industriales.

Ferrocarriles
Aplicaciones ferroviarias – Aparatos de telecomunicaciones y señalización.

Subestaciones
Sistemas y redes de comunicaciones en subestaciones eléctricas.

Westermo
Una combinación de equipos para entornos residenciales, industriales y ferroviarios, con el añadido de la experiencia derivada de los productos Westermo ya instalados.

Ensayo	Puerta	Westermo	
		Nivel	Criterios
Emisión			
Radiada	Caja	30/37 dB (µV/m)	Clase B
Conducida	Alim. CA	66-56/56/60 Qp dB (µV)	Clase B
	Alim. CC	66-56/56/60 Qp dB (µV)	Clase B
Inmunidad			
Descargas electrostáticas	Contacto caja	± 6 kV	B
	Aire caja	± 8 kV	B
Inmunidad a campos radiados	Caja	20 V/m 1 kHz 80% AM 20 V/m 200 Hz pulso	A A
Transitorios eléctricos rápidos	Señal	± 2,0 kV	A
	Alim. CA	± 2,0 kV	A
	Alim. CC	± 2,0 kV	A
Ondas de choque	Señal LE Señal LL	± 2,0 kV ± 2,0 kV	B B
	Alim. CA LE Alim. CA LL	± 2,0 kV ± 2,0 kV	B B
	Alim. CC LE Alim. CC LL	± 2,0 kV ± 2,0 kV	B B
Campos de radio-frecuencia conducidos	Señal	10 V 1 kHz 80%AM	A
	Alimentación	10 V 1 kHz 80%AM	A
Campos magnéticos a frecuencia de red	Caja	100 A/m 50 Hz	A
Campos magnéticos pulsados	Caja	300 A/m 6,4/16 µs	–
Alimentación CA*	Alimentación	30% 10/500 ms 60% 100/1000 ms Interrup. 10/5 ms	B B B
Alimentación CC	Alimentación	30% 10 ms 60% 10 ms Interrup. 10/100 ms 20% por encima/debajo de la tensión nominal	B B
Armónicos	Señal LE Señal LL	– –	– –
	Alim. LE Alim. LL	– –	– –
Perturbaciones 50 Hz**	Señal LE Señal LL	10/100 V 250 V	A A

* Fallos, fluctuaciones, cortes y microcortes en la alimentación.

** Modo común o diferencial conducido.

Criterios: clasificación del rendimiento

Criterio A: Rendimiento normal dentro de los límites establecidos (definidos en las especificaciones del ensayo).

Criterio B: Parada temporal o pérdida de rendimiento que se corrige por sí sola cuando desaparece la perturbación y de la que el equipo objeto del ensayo se recupera totalmente sin necesidad de intervención humana.

Criterio C: Parada temporal o pérdida de rendimiento cuya recuperación requiere intervención humana.

Ensayo	Puerta	Residencial		Industrial		Ferrocarriles		Subestaciones	
		Nivel	Criterios	Nivel	Criterios	Nivel	Criterios	Nivel	Criterios
Emisión									
Radiada	Caja	30/37 dB (µV/m)	Clase B	40/47 dB(µV/m)	Clase A	40/47 dB(µV/m)	Clase A	30/37 dB(µV/m)	Clase A y B
Conducida	Alim. CA	66-56/56/60 Qp dB (µV)	Clase B	79/73 Qp dB(µV)	Clase A	79/73 Qp dB(µV)	Clase A	66-56/56/60 Qp dB(µV)	Clase A y B
	Alim. CC	–	–	–	–	79/73 Qp dB(µV)	Clase A	–	–
Inmunidad									
Descargas	Contacto caja	± 4 kV	B	± 4 kV	B	± 6 kV	B	± 6 kV	A***
electrostáticas	Aire caja	± 8 kV	B	± 8 kV	B	± 8 kV	B	± 8 kV	A***
Inmunidad a campos radiados	Caja	3 V/m 1 kHz 80% AM	A	10 V/m 1 kHz 80% AM	A	20 V/m 1 kHz 80% AM	A	10 V/m 1 kHz 80% AM	A
						20 V/m 200 Hz pulso	A		
Transitorios eléctricos rápidos	Señal	± 0,5 kV	B	± 1,0 kV	B	± 2,0 kV	A	± 2,0 kV	A***
	Alim. CA	± 1,0 kV	B	± 2,0 kV	B	± 2,0 kV	A	± 4,0 kV	A***
	Alim. CC	± 0,5 kV	B	± 2,0 kV	B	± 2,0 kV	A	± 4,0 kV	A***
Ondas de choque	Señal LE Señal LL	± 0,5 kV –	B	± 1,0 kV –	B –	± 2,0 kV ± 2,0 kV	B B	± 4,0 kV ± 4,0 kV	A*** A***
	Alim. CA LE Alim. CA LL	± 2,0 kV ± 1,0 kV	B B	± 2,0 kV ± 1,0 kV	B B	± 2,0 kV ± 2,0 kV	B B	± 4,0 kV ± 4,0 kV	A*** A***
	Alim. CC LE Alim. CC LL	± 0,5 kV ± 0,5 kV	B B	± 0,5 kV ± 0,5 kV	B B	± 2,0 kV ± 2,0 kV	B B	± 4,0 kV ± 4,0 kV	A*** A***
Campos de radio-frecuencia conducidos	Señal	3 V 1 kHz 80%AM	A	10 V 1 kHz 80%AM	A	10 V 1 kHz 80%AM	A	10 V 1 kHz 80%AM	A
	Alimentación	3 V 1 kHz 80%AM	A	10 V 1 kHz 80%AM	A	10 V 1 kHz 80%AM	A	10 V 1 kHz 80%AM	A
Campos mag. a frec. de red	Caja	3 A/m 50 Hz	A	30 A/m 50 Hz	A	100 A/m 50 Hz	A	100 A/m 50 Hz	A
Campos magnéticos pulsados	Caja	– 6,4/16 µs	–	–	–	300 A/m	B	–	–
Alimentación CA*	Alimentación	30% 0,5 s 60% 100 ms Interrup. 5 s	B C C	30% 10 ms 60% 0,1/1 s Interrup. 5 s	B C C	–	–		
Alimentación CC	Alimentación	–	–	–	–	–	–	Interrup. 10 ms	A
								Interrup. arbitraria	C
Armónicos	Señal LE Señal LL	– –	– –	– –	– –	– –	– –	2,5 kV 1,0 kV	A*** A***
	Alim. LE Alim. LL	– –	– –	– –	– –	– –	– –	2,5 kV 1,0 kV	A*** A***
Perturba-ciones 50 Hz**	Señal LE Señal LL	– –	– –	– –	– –	– –	– –	30 V Cont. 300 V 1 s 250 V	A A

* Fallos, fluctuaciones, cortes y microcortes en la alimentación.

** Modo común o diferencial conducido.

*** Cuando se produce una interferencia en la comunicación, el error se acepta si no se producen retrasos ni se pierden datos críticos. No se permiten cambios de estado en las salidas eléctricas, mecánicas y de comunicación, incluidas las de alarma y estado.

EN 61000-4-3 Compatibilidad electromagnética (CEM).
Técnicas de ensayo y medición. Ensayo de inmunidad a los campos electromagnéticos, radiados y de radiofrecuencia.

- Método de ensayo de la inmunidad del equipamiento eléctrico a los campos electromagnéticos, radiados y de radiofrecuencia. Establece varios niveles y métodos de ensayo.

EN 61000-4-4 Compatibilidad electromagnética (CEM).
Técnicas de ensayo y medición. Ensayo de inmunidad a los transitorios rápidos en ráfagas.

- Método de ensayo de la inmunidad del equipamiento eléctrico a los transitorios rápidos en ráfagas. Establece varios niveles y métodos de ensayo.

EN 61000-4-5 Compatibilidad electromagnética (CEM).
Técnicas de ensayo y medición. Ensayo de inmunidad a las ondas de choque

- Método de ensayo de la inmunidad del equipamiento eléctrico a las ondas de choque causadas por sobretensiones de tipo rayo o de tipo maniobra. Establece varios niveles de ensayo que se corresponden con diferentes condiciones de instalación y entorno.

EN 61000-4-6 Compatibilidad electromagnética (CEM).
Técnicas de ensayo y medición. Inmunidad a las perturbaciones conducidas, inducidas por campos de radiofrecuencia.

- Método de ensayo de la inmunidad del equipamiento eléctrico a las perturbaciones conducidas, inducidas por campos de radiofrecuencia, dentro del rango de frecuencias de 9 kHz a 80 MHz. Establece varios niveles y métodos de ensayo.

EN 61000-4-8 Compatibilidad electromagnética (CEM).
Técnicas de ensayo y medición. Ensayo de inmunidad a los campos magnéticos a frecuencia de red.

- Método de ensayo de la inmunidad del equipamiento eléctrico a los campos magnéticos a frecuencia de red. Establece varios niveles de ensayo que se corresponden con diferentes condiciones de instalación y entorno.

EN 61000-4-11 Compatibilidad electromagnética (CEM).
Técnicas de ensayo y medición. Ensayos de inmunidad a fallos, fluctuaciones, cortes y microcortes en la alimentación.

- Método de ensayo de la inmunidad del equipamiento eléctrico a los fallos, fluctuaciones, cortes y microcortes en la alimentación. Establece varios niveles y métodos de ensayo.

Condiciones de seguridad

	Requisito			
Factor	**Severidad**	**Norma**	**Comentarios**	**Referencia**
Seguridad eléctrica	Equipos de tecnología	EN 60 950 de la información		**Apartado 1.6**
Vida útil	10 años			
Conexión eléctrica	Permanentemente conectado			
Accesibilidad	Ubicación de acceso restringido		Acceso: personal técnico y herramientas	
Mantenimiento	No			
Circuito de aislamiento	 A circuito(s)		 Rigidez dieléctrica	
Alimentación Alimentación AT SELV TNV-1 TNV-1 TNV-3	Todos los demás Todos los demás TNV-1, TNV-3 TNV-3 TNV-1 TNV-3		≥1 kVCA 3 kVCA 1 kVCA 1 kVCA 1 kVCA 1 kVCA	 **Apartado 2.3** **Apartado 2.4** **Apartado 2.5**

Condiciones de instalación

Instalación	**Cat. inst.**	**Tipo de cable**	**Puerto**	**Comentarios**
Alimentación	II		Alimentación	
Alimentación (AT)	II		Alimentación	
TNV-3 (<70,7 Vp 120 VCC)	I	No apantallado	Señal simétrica	PSTN o similar
TNV-1 (<42,4 Vp 60 VCC)	I	Par trenzado no apantallado	Señal simétrica	RS-422/485, Ethernet o similar
SELV (<42,4 Vp 60 VCC)	I	No apantallado	Señal	RS-232 o similar

1.6 Seguridad eléctrica

EN 60950 Equipos de tecnologías de la información. Seguridad. Requisitos generales.

- Norma sobre seguridad de los equipos de tecnologías de la información que establece los requisitos para reducir los riesgos de incendio y descarga eléctrica, así como de lesiones al usuario, otras personas y el personal de servicio técnico. Es aplicable tanto a los equipos de tecnologías de la información conectados a la red eléctrica o alimentados por baterías, como a los de conexión directa a la red telefónica, sea cual sea su fuente de alimentación.

Caja

Factor	Severidad	Norma	Comentarios	Referencia
Dimensiones (A x H x P) mm	55 x 100 x 128 35 x 121 x 119	 Carril DIN 1 tarjeta	Carril DIN 2 tarjetas	
Peso en kg (lb)	< 0,6 (<1,3)			
Montaje	Carril DIN 35 mm	EN 60715 (EN 50022)	Montaje a presión	
Grado de protección	IP 20	IEC 529		**Apartado 1.7**
Refrigeración	Convección, espacio: 10 mm (izquierda/derecha) 25 mm (encima/debajo)		Espacio (izquierda/derecha) recomendado para rango de temperaturas completo	
Material de la caja	PC / ABS			
Clase de resistencia al fuego	Clase de inflamabilidad V-0	UL 94		**Apartado 1.8**

1.7 Grado de protección

IEC 529 Grados de protección proporcionados por las envolventes (Código IP)

- Clasificación del grado de protección proporcionado por las envolventes (de los materiales eléctricos). Tipo de protección:
- Protección de las personas contra tensiones peligrosas dentro del equipo.
- Protección del interior del equipo contra la penetración de cuerpos sólidos extraños.
- Protección del interior del equipo contra daños provocados por la penetración del agua.

Así por ejemplo, el grado de protección IP 21 proporciona:

- Protección contra el acceso a partes en tensión
- Protección contra la penetración de cuerpos sólidos extraños de diámetro ≥12,5 mm.
- Protección contra la penetración de agua por caída vertical de gotas de agua.

1.8 Inflamabilidad

UL 94 Norma sobre la inflamabilidad de los materiales plásticos empleados en componentes de dispositivos y aparatos

- Establece los métodos para medir y describir las características de inflamabilidad de los materiales de muestra, expuestos al calor o las llamas de forma controlada en laboratorio.

2 Definiciones

2.1 Rango de tensiones nominales

- Rango de tensiones especificado por el fabricante.

2.2 Rango de tensiones de funcionamiento

- Rango de tensiones a las que, en las condiciones especificadas, puede trabajar el dispositivo. Corresponde al rango de tensiones nominales, más las tolerancias por encima y por debajo de dicho rango.

2.3 SELV

- Circuito secundario diseñado y protegido de tal modo que, en condiciones normales y de primer fallo, sus tensiones no superan el valor de seguridad.

2.4 TNV-1

- Circuito secundario cuyas tensiones de funcionamiento normal no superan los límites de un circuito SELV en condiciones normales y en el que se pueden producir sobretensiones procedentes de las redes de telecomunicaciones.

2.5 TNV-3

- Circuito secundario cuyas tensiones de funcionamiento normal superan los límites de un circuito SELV en condiciones normales y en el que se pueden producir sobretensiones procedentes de las redes de telecomunicaciones.

La transmisión de datos...

...es imprescindible para aumentar la productividad

Con el aumento de la automatización se ha hecho cada vez más necesario contar con una transmisión de datos fiable entre los sistemas y unidades de control y los de producción y medición. Como resultado, la transmisión de datos se ha convertido en un verdadero «sistema nervioso», imprescindible para aumentar la eficacia y la competitividad, que alcanza a todos los ámbitos, desde la fabricación hasta la instalación y el transporte, o el mantenimiento.

Interfaces

Llegar a un acuerdo sobre el tipo de señal y los métodos de conversión y transmisión no es suficiente. Además hay que ponerse de acuerdo en el tipo de conector y los niveles de tensión que debe soportar. En otras palabras: hay que normalizar las interfaces física y eléctrica, y también la interfaz lógica, que define el significado de la señal.
Para controlar el modo en que se crean las señales y se inician y terminan las transmisiones, el orden de transmisión y envío, el método de acuse de recibo de los mensajes, etc., hace falta un protocolo, y hay muchos diferentes entre los que elegir: PROFIBUS, Comli, Modbus, etc.

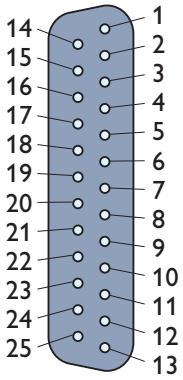
Interfaz física	define la manera en que se conectan los equipos y el diseño del conector.
Interfaz eléctrica	define los niveles eléctricos y lo que denotan (unos y ceros).
Interfaz lógica	define el significado de las señales.

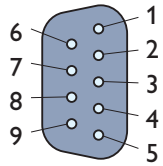
Interfaces más comunes

La interfaz más extendida de transmisión de datos por el puerto serie del equipo informático es RS-232/V.24, que normalmente utiliza un conector sub-D de 9/25 patillas. Según las recomendaciones de la norma RS-232/V.24, el cable entre los dispositivos conectados no debe superar los 15 metros de longitud. No obstante, se pueden lograr distancias de transmisión mayores utilizando diferentes módems, en función del medio de transmisión disponible (por ejemplo, fibra óptica, cobre o circuito de telecomunicaciones). En principio, la norma europea V.24 (del CCITT) y la americana RS-232-C (de la UIT-T) son idénticas (consulte la tabla de la página 25). En la norma europea, V.24 describe la interfaz física, mientras que V.28 corresponde a la interfaz eléctrica. Por este motivo, a veces se hace referencia a ella con el nombre de V.24/V.28.
La interfaz describe y define las patillas del conector, las señales y los niveles de tensión admisibles.

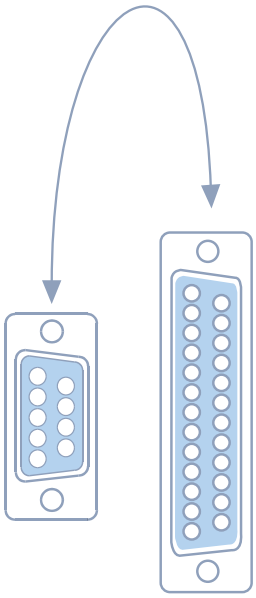
Señales de V.24/RS-232-C

Patilla 9/25		V.24 Código	RS-232 Código	Señal	Descripción	Dirección DCE
	1	**101**	**AA**	**GND**	**Tierra de protección**	–
3	**2**	**103**	**BA**	**TD**	**Datos transmitidos**	**E**
2	**3**	**104**	**BB**	**RD**	**Datos recibidos**	**S**
7	**4**	**105**	**CA**	**RTS**	**Petición de transmitir**	**E**
8	**5**	**106**	**CB**	**CTS**	**Permiso para enviar**	**S**
6	**6**	**107**	**CC**	**DSR**	**Conjunto de datos listo**	**S**
5	**7**	**102**	**AB**	**SG**	**Retorno común**	–
1	**8**	**109**	**CF**	**DCD**	**Detector de la portadora de datos**	**S**
	9	–	–		puede ser de + 12 V	–
	10	–	–		puede ser de -12 V	–
	11	126	SCF	STF	Selección de la frecuencia de transmisión	**E**
	12	122	SCB		DCD secundaria	**S**
	13	121	SBA		CTS secundaria	**S**
	14	118	SBA		TD secundaria	**E**
	15	**114**	**DB**	**TC**	**Reloj de transmisión**	**S**
	16	119	SBB		RD secundaria	**S**
	17	**115**	**DD**	**RC**	**Reloj de recepción**	**S**
	18	–	–		–	–
	19	120	SCA		RTS secundaria	**E**
4	**20**	**108/2**	**CD**	**DTR**	**Terminal de datos preparado**	**E**
	21	110	CG	SQD	Detección de calidad de la señal	**S**
9	**22**	**125**	**CE**	**RI**	**Indicador de llamada**	**S**
	23	111	CH/CI		Selector de velocidad de la señal de datos	**S**
	24	**113**	**DA**	**EC**	**Reloj externo**	**E**
	25	133	–	RFR	Preparado para recibir	**E**





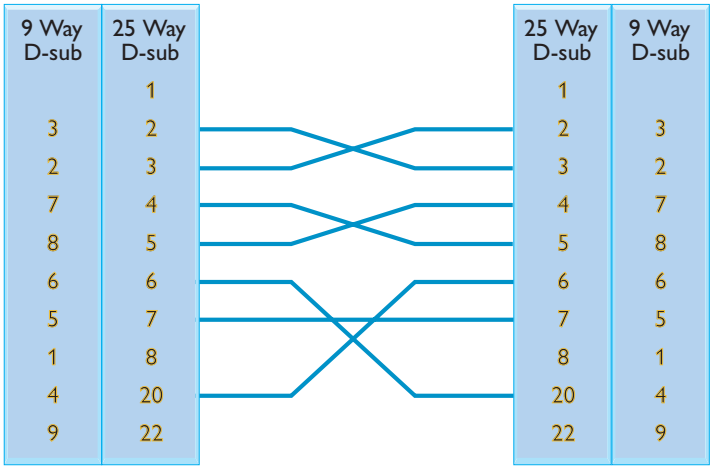
Las señales más comunes en la transmisión de datos local mediante módems de corto alcance son las resaltadas en negrita. La indicación **E/S** describe la dirección en relación con el módem (DCE): **E** es una entrada y **S** una salida. Así, la señal TD (datos transmitidos) es una salida en un DTE y una entrada en un DCE. La definición de DCE y DTE suele dar lugar a confusión cuando ambos elementos están conectados a equipos RS-232 (consulte la página 26).



Configuración de cable

Las figuras muestran cómo se conectan los conectores sub-D de 9/25 patillas en todas las combinaciones de unidades DTE y DCE.

DTE a DTE o DCE a DCE



DTE a DCE

Clave de las señales más importantes

Explicación de las señales más importantes

GND	Tierra de protección	La patilla nº 1 está reservada para la tierra de protección entre los dispositivos.
SG	Retorno común	Es una señal de referencia y en V.24 debe estar siempre conectada a la patilla 7 (25 patillas) o a la patilla 5 (9 patillas).
TD	Datos transmitidos	Es una señal de envío de datos desde un DTE a un DCE.
RD	Datos recibidos	Es una señal de envío de datos desde un módem o un DCE a un DTE.
RTS	Petición de transmitir	Constituye una solicitud de transmisión de datos enviada por un DTE. El dispositivo espera la señal de respuesta CTS.
CTS	Permiso para enviar	Señal de respuesta del DCE que autoriza al DTE a transmitir los datos.
DSR	Conjunto de datos listo	Señal que envía un DCE para indicar que el dispositivo está encendido, que ha establecido la conexión y que está preparado.
DTR	Terminal de datos preparado	Esta señal es equivalente a la anterior (DSR), pero la emite el DTE.
DCD	Detección de portadora de datos	Señal de salida que envía el DCE para indicar que hay portadora disponible entre los DCE y que la conexión está preparada para la transmisión.
EC	Reloj externo	Esta señal se utiliza en la transmisión síncrona, cuando es necesario sincronizar los datos. La señal es la entrada al DCE.
TC	Reloj de transmisión	Transmite el reloj DCE en los sistemas síncronos.
RC	Reloj de recepción	Señal de reloj que recibe el DTE para descodificar los datos.
RI	Indicador de llamada	Señal de salida que emite el módem para indicar que ha recibido una señal de llamada.

ASCII

ASCII es la abreviatura de American Standard Code for Information Interchange (estándar americano de codificación para el intercambio de información). Existen diferentes versiones de este código para distintos idiomas, así como un código ASCII extendido que utiliza el octavo bit de datos.

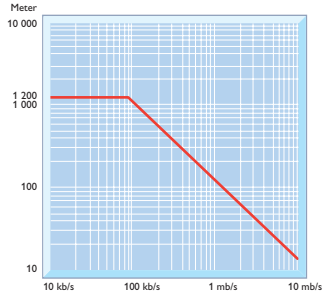
BINARY				b_6	0	0	0	0	1	1	1	1
				b_5	0	0	1	1	0	0	1	1
				b_4	0	1	0	1	0	1	0	1
b_3	b_2	b_1	b_0	**HEX**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	0	0	**0**	NUL	DLE	SP	0	@ / É	P	` / é	p
0	0	0	1	**1**	SOH	DC_1	!	1	A	Q	a	q
0	0	1	0	**2**	STX	DC_2	"	2	B	R	b	r
0	0	1	1	**3**	ETX	DC_3	#	3	C	S	c	s
0	1	0	0	**4**	EOT	DC_4	$ / €	4	D	T	d	t
0	1	0	1	**5**	ENQ	NAK	%	5	E	U	e	u
0	1	1	0	**6**	ACK	SYN	&	6	F	V	f	v
0	1	1	1	**7**	BEL	ETB	'	7	G	W	g	w
1	0	0	0	**8**	BS	CAN	(	8	H	X	h	x
1	0	0	1	**9**	HT	EM	)	9	I	Y	i	y
1	0	1	0	**A**	LF	SUB	*	:	J	Z	j	z
1	0	1	1	**B**	VT	ESC	+	;	K	[/ Ä	k	{ / ä
1	1	0	0	**C**	FF	FS	,	<	L	\ / Ö	l	| / ö
1	1	0	1	**D**	CR	GS	-	=	M	] / Å	m	} / å
1	1	1	0	**E**	SO	RS	.	>	N	^ / Ü	n	~ / ü
1	1	1	1	**F**	SI	US	/	?	O	_	o	DEL

Interfaces industriales

RS-422

RS-422 es una norma excelente para el sector industrial, puesto que esta interfaz permite crear buses de datos, normalmente multipunto, entre los ordenadores centrales y varias subestaciones. Equilibrada y relativamente inmune a las interferencias, la interfaz invierte la polaridad en el par dependiendo de si está transmitiendo un uno o un cero. La especificación original de la norma RS-422 prevé la transmisión de datos desde un maestro a 10 esclavos, que solamente pueden recibir. Nosotros utilizamos los circuitos de excitación para RS-485, interfaz en la que el transmisor puede comunicarse con 32 unidades y gestionar señales «triestado», lo que significa que podemos diseñar aplicaciones multipunto por conexiones de 2 y 4 hilos.

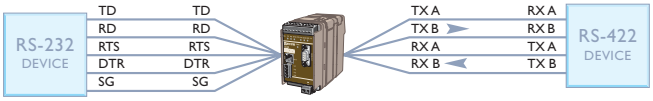
La distancia máxima recomendada es de 1.200 m a una velocidad de transmisión de 100 kbit/s. Los circuitos de excitación admiten velocidades de transmisión de hasta 10 Mbit/s, pero entonces la distancia de transmisión desciende a 20 m. La interfaz RS-422 se puede integrar con la RS-485 y la RS-232/V.24 utilizando un convertidor.



RS-485: Distancias de transmisión

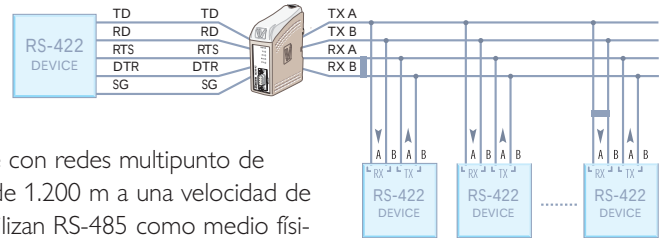
RS-422 a 4 hilos

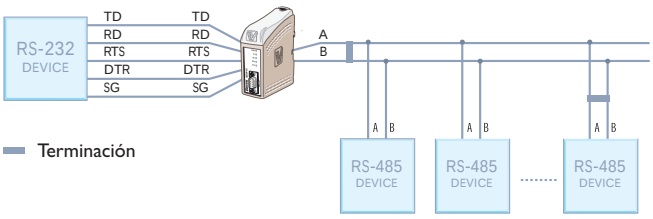
En los sistemas RS-422 a 4 hilos, el transmisor maestro se puede activar/encender en cualquier momento, dependiendo de la actividad de los esclavos. Esta norma permite comunicaciones dúplex simultáneas.

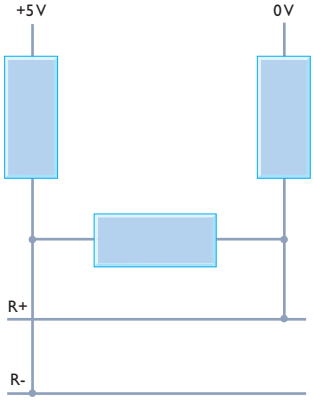


RS-485

La interfaz RS-485 es una evolución de la RS-422 y cada vez se utiliza más como norma en diferentes equipos. Su principal ventaja es que soporta comunicaciones por 2 hilos, en las que el transmisor y el receptor pueden invertir la dirección de transmisión. Diseñada para buses de datos de hasta 32 dispositivos, esta interfaz es compatible con redes multipunto de tipo maestro/esclavo. La distancia máxima recomendada es de 1.200 m a una velocidad de transmisión de 100 kbit/s. Muchas interfaces normalizadas utilizan RS-485 como medio físico, por ejemplo, PROFIBUS, Interbus-S y Bitbus.





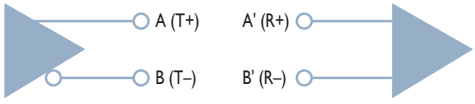


Terminación y sistema a prueba de fallos

Para terminar la línea conviene utilizar una resistencia de valor equivalente al de impedancia característica de la línea, esto es, unos 120 ohmios. Además hay que prever una terminación a ambos extremos del bus, pues de este modo se evitan las reflexiones en el cable. En cuanto al sistema a prueba de fallos («fail-safe»), consiste en una resistencia montada en cada hilo entre el punto positivo de la alimentación, por un lado, y el punto de 0 V, por el otro, con el fin de llevar la línea a un nivel pasivo predeterminado. De no hacerse así se producirían fluctuaciones en la línea, y las perturbaciones resultantes podrían interpretarse como datos.

Polaridad

Es muy importante interconectar el transmisor y el receptor con la polaridad adecuada. Sabemos por experiencia que, cuando se conectan equipos de distintos fabricantes, las normas se pueden interpretar de manera distinta. En efecto, si se produce un error de polaridad en relación con otro equipo, éste no interpretará bien los datos. De conformidad con la norma, el transmisor se designa como A y B, y se conecta a A´ y B´. Nosotros hemos decidido cambiar esta designación por otra más clara: T+, T–, R+ y R- (es decir, transmisión/recepción, + y –).



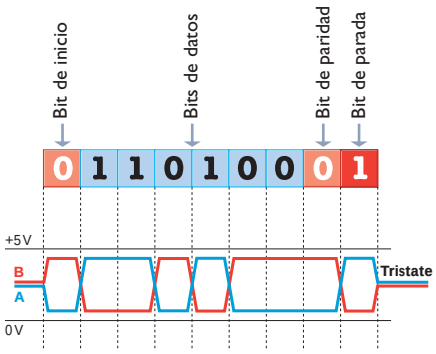
Convertidor RS-232/V.24 a RS-422/485 – Soporte de RTS

En las redes multipunto, los sistemas con convertidores RS-422/485 no admiten más de un transmisor activo simultáneamente en el bus. Los transmisores del resto de dispositivos tienen que estar en modo «triestado», es decir, pasivo. Para lograrlo, es preciso poder controlar los equipos conectados con una señal de hardware. Por lo general, se utilizan señales RTS y DTR. De este modo, cuando un dispositivo desea enviar datos por el bus, primero ha de configurar su señal RTS o DTR a un nivel alto, para que el convertidor active su transmisor y poder transmitir los datos. Cuando no se dispone de señal de hardware se puede utilizar un convertidor especial que activa el transmisor del dispositivo tan pronto como se envían datos por RS-232, y que lo desactiva en cuanto finaliza la transmisión.

Instalación de RS-422 y RS-485

Recomendaciones generales de instalación

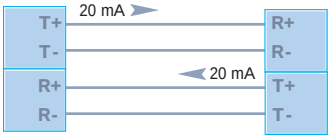
- Hay que utilizar par trenzado.
- No se pueden montar redes en estrella y la distancia entre el bus y el dispositivo no debe superar los 30 cm.
- Hay que terminar los receptores situados en los extremos del bus con una resistencia de 120 ohmios.
- La conexión RS-232/V.24 no debe tener más de 15 m de longitud.
- RS-422/485 admite distancias de transmisión de hasta 1.200 m a 100 kbit/s, aunque se pueden alcanzar distancias mayores reduciendo la velocidad de transmisión.



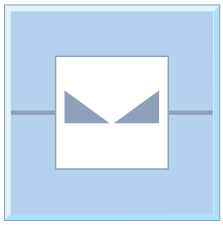
Distancia de transmisión y módems de corto alcance

Como ya hemos mencionado anteriormente, la norma RS-232/V.24 recomienda que el cableado no supere los 15 metros aproximadamente. Para poder establecer enlaces más largos se utilizan módems de corto alcance, que convierten las señales RS-232/V.24 en señales eléctricas y ópticas definidas adecuadas para la transmisión a grandes distancias (hasta varios kilómetros), por ejemplo, por cable de 4 hilos o fibra óptica. El módem de corto alcance receptor convierte de nuevo los datos recibidos en señales RS-232/V.24. El módem debe utilizar una norma común y una interfaz idéntica para las transmisiones por cable.

Bucle de corriente de 20 mA (TTY)



La técnica del bucle de corriente es la más antigua de todas. En ella, las señales RS-232/V.24 se codifican en un bucle de corriente de 20 mA que permite pasar o interrumpe la corriente en un par.
Para el paso de corriente por cada par, el transmisor puede estar activo y el receptor pasivo, o viceversa. El bucle de corriente garantiza una comunicación fiable pero, al no ser simétrico (consulte la página 40), es relativamente sensible a las interferencias. Además, los equipos pueden tener problemas porque la técnica del bucle de corriente no está normalizada.

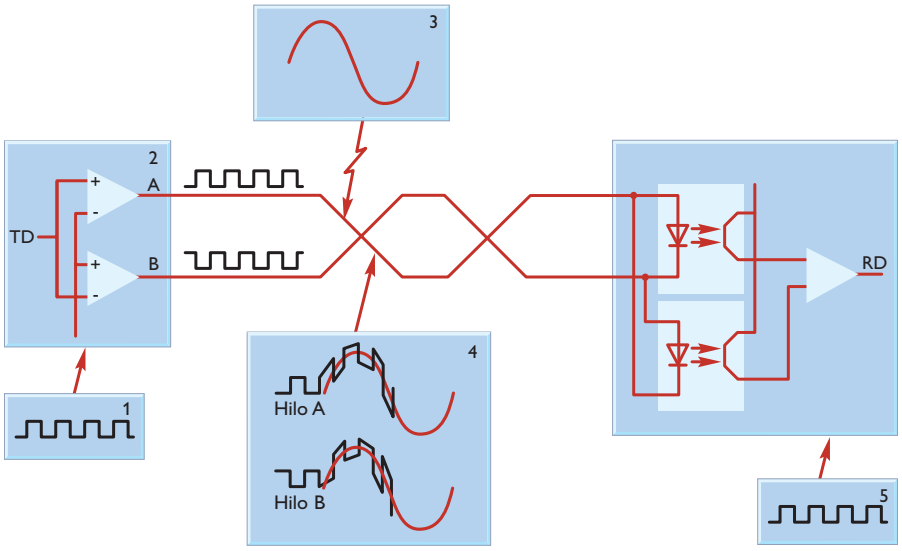


Bucle de corriente simétrica de 10 mA (W1)

En Westermo hemos desarrollado una tecnología de transmisión propia para los módems de corto alcance que garantiza la comunicación a mayor distancia y en entornos con niveles elevados de interferencias. Esta tecnología se basa en la transformación de las señales en un bucle de corriente simétrica de ±10 mA, en el que la dirección de la corriente se decide en el par de hilo, dependiendo de si la señal enviada por la interfaz RS-232/V.24 es de alto o de bajo nivel. La línea del transmisor está alimentada a ±10 mA, y el receptor cuenta con un optoacoplador para la detección de las señales, que además proporciona aislamiento galvánico completo entre los módems. La corriente fluye continuamente en un solo sentido, aunque no haya ningún equipo conectado del lado de la interfaz RS-232/V.24, salvo cuando el transmisor se controla/activa mediante una señal de sincronización. Se trata de una técnica probada y de confianza que a lo largo de los años ha demostrado una gran fiabilidad e inmunidad a las interferencias y que admite distancias de transmisión de hasta 18 km.

Por tanto, el bucle de corriente de 10 mA es menos sensible a las fuentes de interferencias externas.

Comparado con el bucle de corriente asimétrica, el bucle de corriente simétrica es considerablemente menos sensible a las perturbaciones externas derivadas de las diferencias de potencial, aun en caso de interferencia en la línea. La figura que se muestra a continuación ofrece una explicación gráfica.



1. Los datos se envían al transmisor.
2. Los datos que circulan por el hilo A se invierten respecto de los que van por el hilo B.
3. La línea sufre interferencias.
4. Los datos transmitidos se superponen a la interferencia.
5. Los datos que llegan al receptor coinciden totalmente con los enviados por el transmisor (1).

Redes

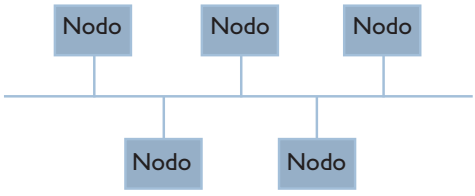
La aparición de las redes locales se produjo en los años 80, inicialmente mediante mainframes centrales o miniordenadores con terminales conectados en estrella. El establecimiento de las redes trajo además consigo la necesidad de disponer de transmisiones de datos seguras y fiables.

La transmisión requiere un transmisor, un receptor, un medio, datos y un protocolo. El transmisor, el receptor y el medio precisan una especificación sobre los dispositivos físicos (cómo conectarlos en red, etc.). Por su parte, el protocolo gestiona las reglas que regulan la transferencia (este punto se aborda en detalle más adelante).

Las redes locales no sólo están pensadas para transmitir datos en las oficinas, sino también en industrias, hospitales, explotaciones mineras o centros de control del tráfico. Contar con una red de comunicaciones potente y fiable es uno de los requisitos básicos para el desarrollo de las empresas y organismos, pues gracias a ellas éstos pueden:

- *Compartir información:* las bases de datos comunes, el correo electrónico y la posibilidad de compartir archivos aumentan la eficacia en el trabajo.
- *Compartir recursos:* a través de la red, varios usuarios pueden utilizar valiosos recursos compartidos, como impresoras de color o aplicaciones informáticas instaladas en un servidor.
- *Garantizar la seguridad:* gracias a los privilegios de acceso a la red para usuarios o grupos de usuarios, es posible controlar el acceso a cada aplicación y, de este modo, reforzar la eficacia de la administración centralizada.

En las charlas sobre redes aparece siempre con cierta frecuencia la palabra nodo. Un nodo puede ser, por ejemplo, un ordenador, una impresora o un equipo de comunicación. La diversidad de nodos existentes y el elevado número de funciones que pueden tener asignadas hace necesario normalizar su forma de comunicarse entre sí.



En efecto, del mismo modo que los seres humanos necesitamos hablar la misma lengua para poder entendernos, los equipos de la red también necesitan un idioma común. Para ello se utiliza el protocolo, que determina cómo va a tener lugar la comunicación, qué se va a decir, quién lo va a decir, cuándo y cómo. Los protocolos tienen que estar armonizados, de manera que todos los fabricantes apliquen las mismas normas, que pueden haber sido desarrolladas por empresas individuales (normas de facto) o por organismos oficiales como ISO, ANSI o IEEE.

La calidad de la red depende de diversos factores, entre otros los siguientes:

- La velocidad, que a su vez depende del número de usuarios simultáneos, del medio, del hardware y del software.
- La manera en que tiene lugar la transmisión, si llega al receptor correcto y sólo a ese.
- La calidad de los datos, que exige reducir al mínimo las perturbaciones.
- La velocidad de la red.
- La fiabilidad, es decir, el grado de protección de la red contra los transitorios, las corrientes de fuga y otros fenómenos que pueden perturbar la comunicación.
- La seguridad, esto es, hasta qué punto está protegida contra los virus y cualquier otra forma de ataque externo.

Además, a lo largo de los años se ha ido haciendo cada vez más necesario conectar entre sí las distintas redes locales, con el fin de transmitir datos a otros centros de la empresa y a otras empresas, a escala nacional e internacional. Como resultado, se hace necesario analizar el modo en que los diferentes sistemas y bases de datos de una empresa, repartidos por todo el mundo, se comunican entre sí. Las opciones son muchas:

- LAN (**L**ocal **A**rea **N**etwok): red de área local. Red rápida para comunicaciones locales, por ejemplo, Ethernet.
- MAN (**M**etropolitan **A**rea **N**etwork): red de área metropolitana. Red rápida que abarca una zona geográfica más amplia.
- WAN (**W**ide **A**rea **N**etwork): red de área extensa. Red con una distribución geográfica muy grande; puede ser un país o incluso todo el planeta.
- VAN (**V**alue **A**dded **N**etwork): red de valor añadido. Red que ofrece servicios más amplios que la mera transmisión de datos.
- GAN (**G**lobal **A**rea **N**etwork): red de área global. Red integrada por varias redes locales que pueden estar interconectadas mediante una red MAN o WAN rápida.
- AAN (**A**ll **A**rea **N**etwork): red global. Red que se puede utilizar tanto en redes locales como en redes geográficamente más extensas.

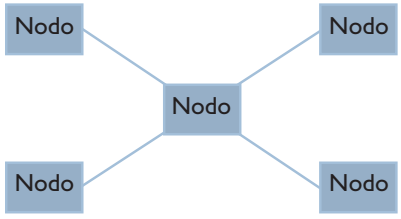
Topología de red

El término topología hace referencia a la estructura de la red, es decir, a la ubicación física y lógica de los nodos. Las topologías básicas son cinco: punto a punto, anillo, estrella, bus y mixta. La elección de la topología es muy importante, porque se trata de una infraestructura que debe durar muchos años y que tiene que gestionar y transmitir datos importantes sin interrupciones ni tiempos de inactividad.
Además, debe ofrecer posibilidades de adaptación y de evolución en función de las necesidades.

Red punto a punto serie

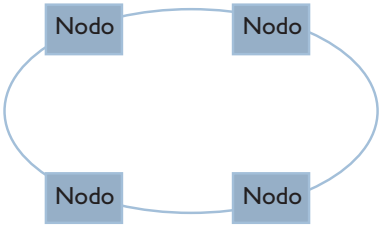
La transmisión de datos punto a punto, esto es, entre dos equipos conectados, es una de las más comunes, tanto en aplicaciones básicas por ejemplo, ordenador a impresora, como en aplicaciones más complejas en las que el administrador asigna permisos a cada usuario en función de los requisitos de seguridad. La interfaz RS-232/V.24 no es recomendable para distancias de transmisión de más de 15 metros, por lo que es habitual utilizar un módem que permite extender la línea hasta 18 km y que, de paso, elimina las perturbaciones.

Red en estrella



Es una red formada por muchos usuarios conectados entre sí punto a punto. Cada dispositivo se comunica con la unidad central por su propia línea. La principal ventaja de este tipo de red es su elevada fiabilidad: si una línea falla, las otras no se ven afectadas. Sin embargo, tiene dos inconvenientes reseñables: requiere más cable, con el consiguiente aumento de los costes, y toda la comunicación debe pasar por la unidad central.

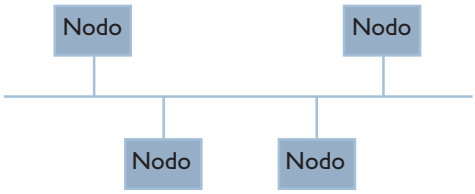
Red en anillo



En este tipo de red todas las unidades están interconectadas formando un círculo cerrado, por lo que todas las transmisiones deben pasar «a través» de todos los dispositivos del anillo para llegar al receptor. Para evitar colisiones, se hace circular por la red una «ranura vacía». El nodo transmisor se asegura de que la ranura está vacía y le adjunta una dirección y los datos. El nodo siguiente comprueba el contenido de la ranura para ver si está dirigido a él y, si el destinatario es otro, la envía al siguiente. Cuando la ranura llega al receptor, éste la vacía, inserta un acuse de recibo y la devuelve a la red. El dispositivo transmisor comprueba que el receptor ha recibido y acusado recibo del mensaje y, a continuación, vuelve a poner la ranura vacía en circulación. La red Token Ring es un ejemplo de red en anillo desde el punto de vista de la señal, conectada físicamente como una red en estrella distribuida. Las redes en anillo ofrecen un gran rendimiento, pero resultan más difíciles de configurar y adaptar que las redes de bus.

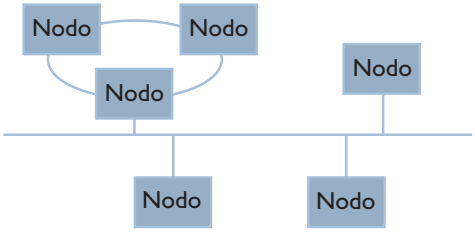
Red de bus

En principio, la red de bus está formada por una línea principal a la que están conectadas como nodos todas las unidades. Todo el tráfico de datos se envía al receptor correspondiente a través del bus. La red de bus tiene que tener definidas normas sobre la manera en que el dispositivo transmisor comprueba si la línea está libre y lo que debe hacer si se produce una colisión con otro mensaje debido, por ejemplo, a una retransmisión diferida. Este tipo de red es fácil de instalar, ampliar y extender. Ethernet y AppleTalk son ejemplos comunes de redes de bus. Uno de sus inconvenientes es que el tráfico se ralentiza cuando los dispositivos que envían datos por la red son muchos. No obstante, la red se puede dividir en varios buses más cortos, que segmentan la red.



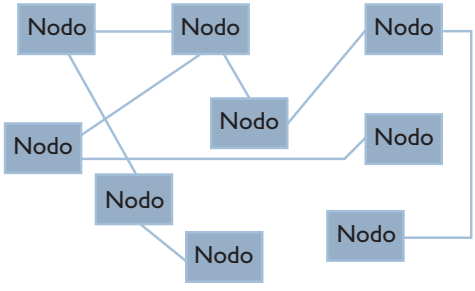
Red mixta

Utilizando diferentes productos de comunicación se pueden crear redes personalizadas que combinen las ventajas de las distintas topologías, incluidas las de rendimiento y fiabilidad. Así, se puede crear una red de bus en estrella distribuida, para conectar varias redes en estrella. Con todo, es importante recordar que cada red necesita un sistema completo de normas de trabajo y de transmisión.



Red en malla

La red en malla es una red interconectada sin una estructura determinada. En una red sin estructura y mal documentada, el riesgo de que se cometa un error que provoque fallos en la transmisión es bastante alto. Por ejemplo, si conectamos otro nodo a la red y, al hacerlo, creamos un bucle, por la red circulará un mensaje de difusión que dará lugar a otros hasta producir una verdadera tormenta de difusiones en la red.

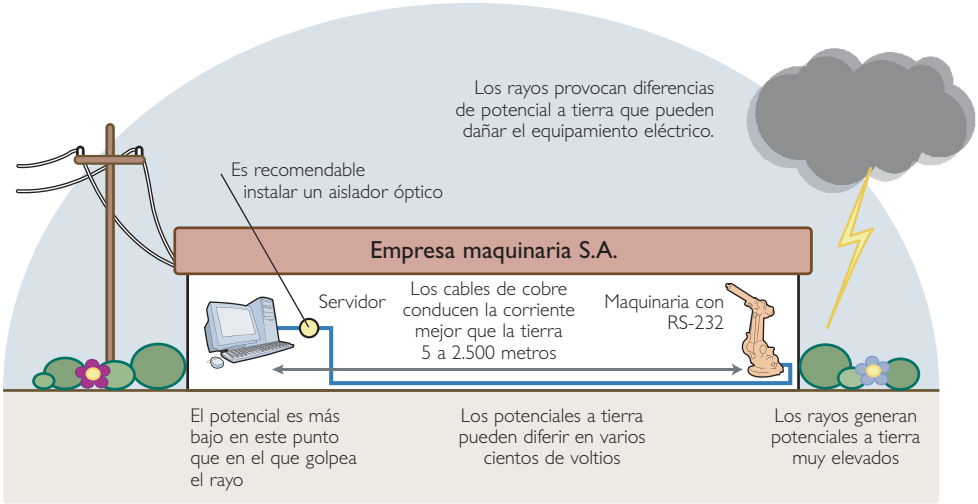


El problema de las interferencias

Por desgracia, disponer de métodos de transmisión adecuados y de la interfaz correcta no resuelve todos los problemas de la transmisión de datos. Aún queda el peor enemigo: la interferencia. Las perturbaciones externas provocan pérdidas de datos, errores de transmisión y, en el peor de los casos, averías en los equipos. Además, la creciente miniaturización de los circuitos y componentes informáticos, y la consiguiente reducción de las tensiones de alimentación, si bien resulta ideal desde el punto de vista energético, acrecienta el problema de las interferencias, pues los hace más sensibles y vulnerables a las sobretensiones. Los estudios demuestran que hasta un 70% de las perturbaciones que sufren los datos se deben a deficiencias en la instalación o a interferencias provocadas por el entorno, los equipos próximos, las máquinas o el cableado. Sólo el 20% se debe a fallos del hardware o el software. Esto quiere decir que los «culpables» casi siempre se encuentran dentro de nuestras paredes o en las proximidades; el resto de las perturbaciones proviene del exterior, como los rayos. El grupo más grande lo forman los transitorios, pulsos de tensión cortos pero intensos en la red. Un equipo informático expuesto a transitorios de 1.000 V a 10 kV durante sólo unas milésimas de segundo está siempre al borde del peligro.

Rayos, maquinaria y tubos fluorescentes

Sabemos que, al golpear, los rayos descargan tensiones muy elevadas y que, al propagarse, éstas dañan las líneas eléctricas y de telecomunicaciones, llegando a provocar incendios en el peor de los casos. Además, aunque el rayo caiga a cierta distancia, los pulsos que descarga se propagan a grandes distancias por la red de cables o debido a las diferencias de potencial existentes entre dos puntos. Por eso a veces las bombillas parpadean aunque la tormenta parezca estar muy lejos.



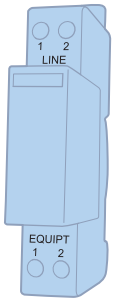
Pero no sólo las tormentas generan transitorios. La bombillas también pueden parpadear cuando una fábrica cercana enciende o apaga su maquinaria, porque estos procesos generan transitorios y picos de tensión en la red.

Con todo, la mayoría de los transitorios tienen su origen dentro del propio recinto. Las máquinas, los equipos y los tubos fluorescentes provocan pulsos de tensión en la red. Los tubos fluorescentes, al apagarse, pueden emitir energía almacenada en forma de transitorios de hasta 3.000 V. El golpe de un rayo cerca de un cable eléctrico puede provocar un transitorio de 6 a 10 kV. Las placas de circuito de telecomunicaciones estándar de los ordenadores están diseñadas para ±12 V, y los transitorios suelen ser el motivo por el que un PC se estropea inexplicablemente o la comunicación se interrumpe temporalmente. Los transitorios son, pues, la principal causa de las perturbaciones. Las interferencias provocadas por fallos en la red, tales como subtensiones, sobretensiones o cortes de electricidad, constituyen únicamente en torno al 10% de los casos.

Protección contra rayos y sobretensiones

Como los rayos y las sobretensiones pueden dañar los equipos de comunicaciones, nuestros clientes a menudo nos preguntan cuál es el método de protección más eficaz. Controlar al cien por cien los efectos de las ondas de choque de tipo rayo es extremadamente complicado; no obstante, se pueden evitar muchos problemas instalando un sistema de protección adecuado. La protección contra este tipo de perturbaciones tiene una doble vertiente: la protección contra las ondas de choque directas y la protección contra las sobretensiones inducidas.

En el primer caso, la protección debe ser capaz de desviar varios cientos de miles de amperios. En el segundo, la cosa es más sencilla, pues en las tensiones inducidas los transitorios son más lentos y la corriente que hay que desviar es muchísimo menor. Como su propio nombre indica, las sobretensiones inducidas se transmiten por inducción, por lo que no es necesario que se produzca un contacto directo. Sin embargo, también son las más frecuentes, pues se producen cada vez que golpea un rayo.



Ejemplos de protección contra las sobretensiones

Interfaz	Tensión nominal
RS-232	12 V
RS-422/RS-485	12 V
W1	24 V
4-20 mA	24 V
Línea dedicada con módem telefónico	24 V
Línea conmutada con módem telefónico	170 V

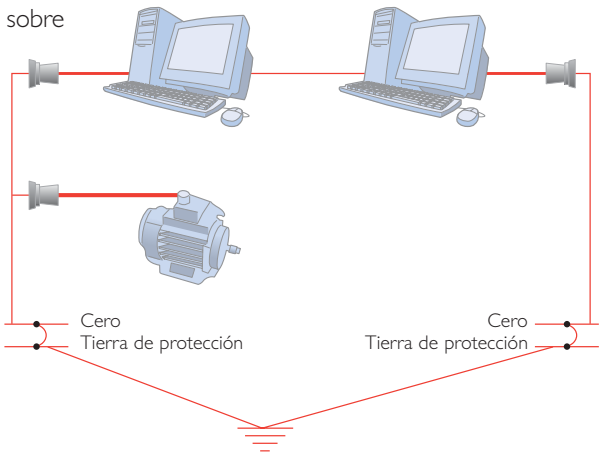
En el mercado existe una gran variedad de sistemas de protección contra las sobretensiones tanto para las líneas de señal/telecomunicaciones como para los módems telefónicos, RS-232, 4–20 mA, RS-485 y otras señales típicas. Estos sistemas incorporan una protección primaria y otra secundaria, adaptada al método de comunicación. Por lo general no requieren mantenimiento, pues vuelven al estado inicial después de desviar el transitorio. De hecho, si no lo hacen lo más probable es que la protección haya fallado por uno de los motivos siguientes:

- El valor de tensión transitoria ha superado la capacidad de la protección (por haber caído el rayo demasiado cerca de la instalación).
- La sobretensión ha durado demasiado (por ejemplo, debido a una conexión directa a 230 V).

Bucles de tierra

Entre las causas más comunes de los errores en la transmisión de datos se encuentran también las diferencias de potencial a tierra y *los bucles de tierra*, sobre todo cuando los equipos de la red reciben la alimentación de paneles de distribución distintos que presentan potenciales a tierra diferentes cuando se conectan a tierra. En estos casos, las corrientes parásitas pueden derivarse a tierra por dos rutas diferentes: por la correcta, a través de la tierra del panel de distribución, o por el retorno común del puerto serie a tierra del otro panel de distribución. Las corrientes de tierra que circulan por la red pueden causar perturbaciones y dañar los circuitos que alimentan la línea. Las redes de comunicaciones están formadas por muchos metros de cables físicos, a menudo canalizados junto a otros cables de electricidad y telecomunicaciones. Todos los cables que conducen electricidad generan un campo electromagnético que afecta tanto a los cables adyacentes como a los que se cruzan con ellos. Juntos, forman *antenas* muy grandes que pueden captar todo tipo de interferencias. Existen varias recomendaciones sobre la manera en que deben conducirse los diferentes tipos de cables para reducir al mínimo las perturbaciones electromagnéticas, pero la manera más sencilla de resolver tanto el problema de los transitorios como el de las diferencias de potencial a tierra es utilizar un módem con *aislamiento galvánico,* pues este tipo de protección aísla eléctricamente los cables y los equipos, sin afectar a la transmisión de señales, y evita que los transitorios, las ondas de choque de tipo rayo y las corrientes de tierra lleguen al equipo.

En el ejemplo, las corrientes de fuga pueden tomar una ruta incorrecta, a través del retorno común de la red informática hasta un panel de fusibles, y generar interferencias.



Reducción de las interferencias

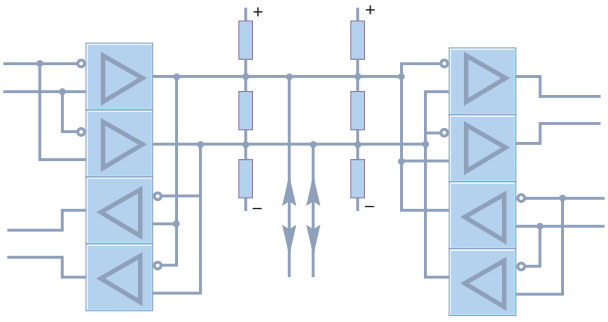
En cualquier sistema, las señales electrónicas son siempre sensibles a las interferencias. Las señales analógicas suelen serlo aún más, porque todos los puntos de la señal transportan información, es decir, amplitud y frecuencia. Incluso las perturbaciones más pequeñas hacen que el receptor interprete lo que le llega de forma incorrecta y cree una salida incorrecta. En cambio, las señales digitales son menos sensibles a las interferencias, ya que tienen solamente dos estados básicos: alto o bajo. No obstante, las interacciones entre la capacidad, la resistencia y la inductancia de los cables utilizados para conducir las señales digitales, así como los efectos del ruido externo, pueden distorsionar la señal hasta el punto de hacerla irreconocible.

Señales simétricas

Las señales simétricas se utilizan para transmitir pulsos a grandes distancias con interfaces diferenciales como RS-422/485 o W1.

Cuando se utilizan protocolos simétricos en cables de par trenzado, los campos inducidos eliminan con gran eficacia la diafonía entre los pares.

En los sistemas asimétricos no se produce este efecto.



Transmisión simétrica rápida

Aislamiento

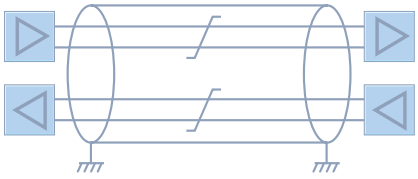
En las transmisiones de datos es esencial aislar galvánicamente los equipos y redes entre sí para evitar la propagación de transitorios y otras formas de interferencias que pueden provocar errores en la transmisión o daños en los equipos.

Para garantizar el aislamiento se pueden utilizar diversos dispositivos, como relés, transformadores, amplificadores de aislamiento y optoacopladores, mientras que para eliminar los transitorios entrantes se pueden instalar componentes de protección tales como varistores, condensadores, filtros RC y diodos Zener.

Westermo utiliza optoacopladores de aislamiento en sus receptores, pues estos dispositivos ofrecen un rendimiento más alto que, por ejemplo, los amplificadores diferenciales. Los transformadores proporcionan aislamiento en las fuentes de alimentación, mientras que los varistores y los diodos Zener se utilizan para eliminar los transitorios.

Redes a tierra

El mejor método general de minimizar las perturbaciones es que el sistema sea de diseño equipotencial, es decir, que todos los edificios, la electrónica, los buses de campo y los dispositivos instalados tengan el mismo potencial a tierra. En la práctica es muy difícil conseguirlo, pero sí se puede lograr un potencial uniforme utilizando conductores de tierra especiales y redes con hilo de guarda. Es importante que la red con hilo de guarda y la tierra de protección estén interconectadas, y que estén tan cerca una de otra como sea posible.

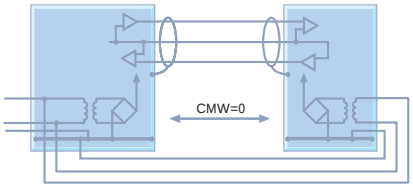


Transmisión de datos a RS-422 a 10 Mbit.

Apantallamiento

Los cables con pantalla simple o doble aumentan la resistencia a las interferencias externas. En circunstancias normales, basta con que la pantalla del cable esté conectada a tierra por un extremo.

Sin embargo, en algunos casos extremos en que el ruido de alta frecuencia es un problema, conviene conectar el cable a tierra por ambos extremos. Con todo, hay que tener en cuenta que este método puede llegar a provocar problemas considerables si los puntos de conexión presentan diferencias de potencial. En efecto, en esos casos la corriente atravesará la pantalla, llevando consigo cualquier ruido al plano de tierra.



Transmisión de datos a RS-232/V.24.

Como alternativa, se puede conectar uno de los extremos de la pantalla directamente a tierra y el otro a través de un condensador pequeño de alta tensión.

Conexiones a corta distancia sin módem

Para poder transmitir datos por RS232/V.24 sin módem, la distancia entre los equipos conectados ha de ser muy pequeña. Los cables tienen que conducirse separados de los demás, pero tan cerca del cable de tierra como sea posible, y los chasis de los dispositivos tienen que interconectarse con cable de cobre para reducir los problemas de ruido CMV (**C**ommon **M**ode **V**oltages, es decir, tensiones de modo común). RS-232/V.24 permite una transmisión de datos lenta hasta una distancia máxima de 15 metros. Si la distancia es mayor, hay que utilizar un módem o un controlador de línea.

Con RS-422 la protección es mayor, pues tanto el transmisor como el receptor son simétricos. En este caso se puede utilizar par trenzado apantallado y los dispositivos, si están separados, deben tener el chasis interconectado y, a ser posible, recibir alimentación de la misma fuente.

Módems telefónicos e interferencias

Cuando se utilizan módems telefónicos en aplicaciones industriales, es importante recordar que se trata de dispositivos muy sensibles a las interferencias, a pesar del aislamiento y de la codificación de las señales. Si el cable no se protege de la manera adecuada, la comunicación puede sufrir perturbaciones y los componentes pueden resultar dañados. El cableado de telecomunicaciones debe estar separado del de procesamiento. Además, en entornos industriales adversos se puede utilizar una combinación de dispositivos de protección para aumentar el nivel de protección.

Cable de fibra óptica

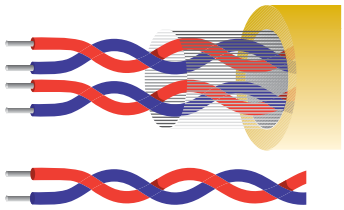
En este contexto, la transmisión de datos por fibra óptica es completamente inmune a las interferencias eléctricas. No obstante, el tipo de cable y la atenuación en los empalmes pueden afectar a la calidad de las comunicaciones.

Tipos de cables de cobre

En la transmisión de datos, el cable físico suele ser el «punto débil». Es el cable el que transporta la señal analógica sensible a las interferencias y el que, en función de su diseño, instalación y longitud, junto con los efectos eléctricos del entorno, determina la velocidad y la calidad de las comunicaciones.

Par trenzado

Es el tipo de cable más común, sencillo y barato, y suele tener 4 hilos. Se trata de hilo de cobre estándar revestido de una funda de plástico, con o sin pantalla de metal protectora. Los hay de distintos tipos y marcas, con diferentes prestaciones que hay que tener en cuenta al diseñar la instalación, y también con diferentes capas de aislamiento, adaptadas a distintos entornos de instalación. Para lograr una transmisión de calidad, hay que tener en cuenta tres factores: la resistencia, la capacidad y la atenuación.



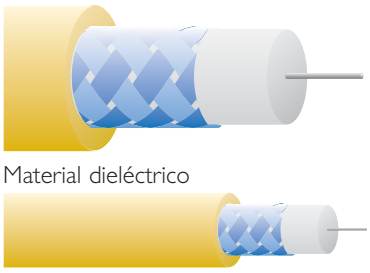
Resistencia Indica la resistencia eléctrica del cable. Se mide en ohmios/km y varía en función del material y la sección del cable. La resistencia del cable aparece indicada en su ficha técnica. En los cables con conductor sólido, el diámetro no debe ser inferior a 0,26 mm^2, y en los de conductor multifilar, éste no debe bajar de 0,2 mm^2. A velocidades de transmisión bajas es la resistencia la que determina los límites.

Capacidad Al estar aislados entre sí, los conductores del cable generan entre ellos un efecto capacitivo. El par trenzado, el material conductor y, en su caso, la pantalla, también influyen en el efecto capacitivo. La capacidad atenúa las señales de manera diferente según la frecuencia, y el valor suele estar situado en 800 Hz. Se mide en pF/m y el valor recomendado para los cables de transmisión es de aproximadamente 50-70 pF/m.
A velocidades de transmisión altas es la capacidad la que determina los límites.

Atenuación Indica la atenuación general que sufre la señal en su recorrido desde el transmisor hasta el receptor a causa del cable. Se expresa en dB/km y aumenta con la frecuencia. Un aumento de 3 dB en la atenuación implica una disminución de la potencia a la mitad.

Atenuación (ejemplos)

150 kHz	8 dB/km
1 MHz	20 dB/km
4 MHz	40 dB/km
10 MHz	65 dB/km
16 MHz	82 dB/km
25 MHz	105 dB/km



Cable coaxial

El cable coaxial está formado por un conductor monofilar de cobre rodeado de una pantalla. Para que la separación entre estos dos elementos sea siempre estable, el espacio va relleno con una capa dieléctrica de plástico aislante. La pantalla se utiliza como protección y para las señales de retorno. El cable coaxial presenta buenas propiedades eléctricas y es adecuado para transmitir datos a gran velocidad. Originalmente, Ethernet utilizaba únicamente cable coaxial de dos tipos: grueso (10Base5) y fino (10Base2). Sin embargo, hoy día Ethernet utiliza cada vez más par trenzado especial (10BaseT). El cable coaxial tiene la ventaja de ser de banda ancha, lo que permite transmitir varios canales simultáneamente (como en la televisión por cable).

Distancia y diseño

No siempre es fácil construir puentes para la transmisión de datos. En efecto, no sólo hay que interconectar diferentes puntos con un medio de transmisión, sino que además éste debe tener capacidad suficiente para la carga de tráfico actual y futura, ser compatible con determinadas velocidades de transmisión, no requerir mantenimiento y resistir el impacto del entorno.

Como todo ello requiere determinar un diseño adaptado a las condiciones específicas de cada aplicación, es imposible proponer uno general válido para todas las áreas. Lo mejor es hablar de las distintas posibilidades con uno o varios expertos para encontrar la solución óptima.

Distancias de transmisión con diferentes tipos de cable y velocidades

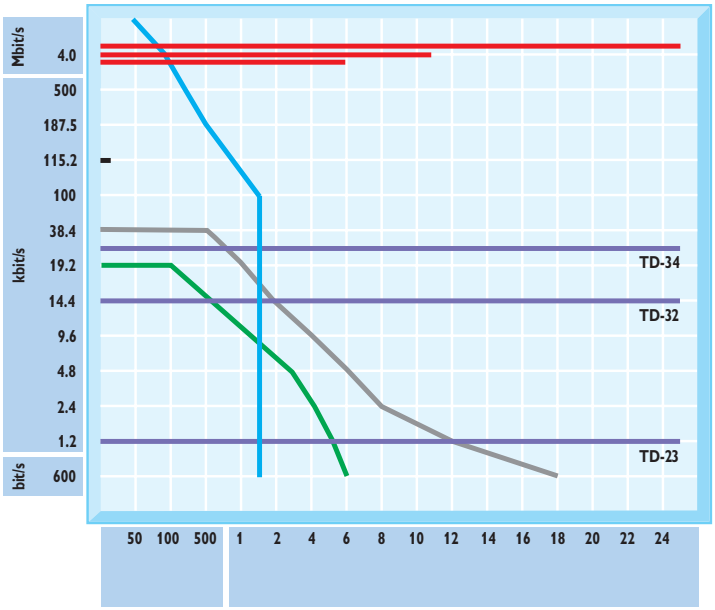
El gráfico que aparece más abajo muestra la distancia de transmisión que se puede obtener con diferentes tipos de cable y velocidades. Las líneas de color negro, azul y verde representan cables de par trenzado de 0,3 mm^2 y 42 pF/m. Dado que la calidad y las dimensiones varían en función del cable de telecomunicaciones, en este caso hemos utilizado un cable muy común en la red telefónica sueca que tiene una sección de 0,2 mm^2 y una atenuación de aproximadamente 1,1 dB/km.

Cálculo de la resistencia

La resistencia del cable, cuando no se conoce, se puede calcular con la siguiente fórmula:
Q = R x A/l
Donde Q es la resistividad del material que se va a utilizar. En los cables de cobre, se puede utilizar 0,017 μ Ωm, o bien 0,017 x 10^{-6}. R es la resistencia en el cable, A es la sección y l la longitud.
Esta fórmula es muy fácil de aplicar en el caso de los conductores sólidos. Si el cable es multifilar, hay que multiplicar la sección del conductor por el número de conductores.
Sección = radio x radio x pi.

Dos maneras de expresar la capacidad

La capacidad se puede expresar en nF/km o en pF/m, que son dos variantes de la misma unidad de medida. nF significa nanofaradio y equivale a 10^{-9} faradios por 1.000 metros, y pF significa picofaradio y equivale a 10^{-12} faradios por metro.

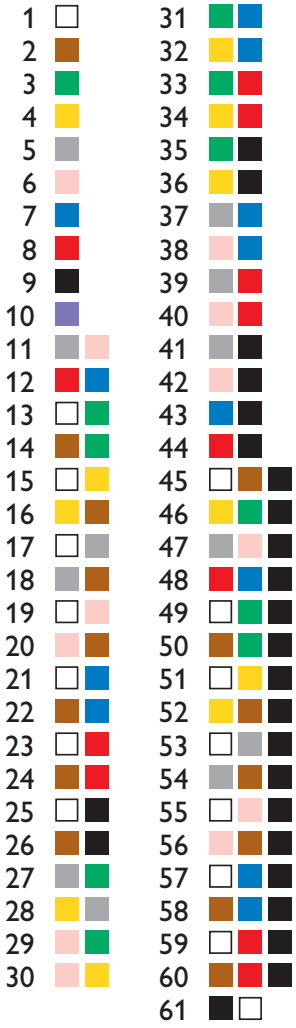


- Línea telefónica dedicada
- Bucle de corriente simétrica de 10 mA (W1)
- Fibra óptica
- RS-422/485
- Bucle de corriente de 20 mA
- RS-232/V.24

Nota: todas las velocidades y distancias se han calculado para cables con valores estándar de resistencia e impedancia.
La distancia de transmisión en las instalaciones puede variar en función de la calidad del cable y de las condiciones del entorno.

Códigos de color

Norma DIN 47100 para cables de datos LiYY y LiYCY. Nº de conductor y color:



Marcado de los cables

El marcado de los cables está regulado en varias normas; la sueca es la norma SEN 241701. Además existe una norma internacional común del CENELEC (Comité Europeo de Normalización Electrotécnica). Los cables pueden ir marcados con un número variable de letras (2 a 5) que tienen el significado siguiente:

Conductor — E D C K P — *Otros*

Aislamiento · *Revestimiento* · *Propiedades*

1ª letra
A *cobre, monofilar*
B *cobre, multifilar*
K *tubo coaxial*
M *cobre, multitrenzado*
R *cobre, multitrenzado extra*
S *cobre, calibre fino*
T *cobre, calibre ultrafino*

2ª letra
D *caucho, cubierta de caucho*
E *caucho de etileno-propileno*
F *caucho de fluorocarburo*
H *caucho de silicona*
I *poliuretano*
K *PVC*
L *plástico de politeno*
M *plástico de polipropileno*
N *poliamida*
T *politetrafluoroetileno (teflón)*
U *plástico de politeno celular*
V *caucho, sin cubierta de caucho*

2ª y 3ª letras
O *caucho resistente a las inclemencias del tiempo y al aceite (caucho de cloropreno)*
S *polietileno clorosulfonado*

3ª letra
C *conductor concéntrico de cobre*
H *tejido trenzado resistente al calor*
I *poliuretano*
J *armado con fleje de acero*
K *cubierta de PVC de sección redonda*
L *plástico de politeno*
N *poliamida*
T *hilo de acero galvanizado con armadura*
U *sin cubierta*
V *caucho*
Y *con aislamiento y funda simple*

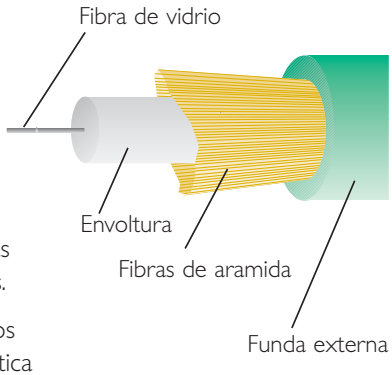
3ª y 4ª letras
A *pantalla de aluminio*
F *cable con pantalla metálica*
P *hilo de acero galvanizado con armadura*

4ª letra
B *conexión o cable para vehículos*
D *funda con refuerzo embutido y conductores sueltos*
H *conductores aislados, cableado alrededor del refuerzo*
K *funda de PVC*
L *funda de PE*
N *funda de PA*
O *funda de caucho resistente a las inclemencias del tiempo y al aceite (caucho de cloropreno)*
T *línea de conexión pesada*
V *cable submarino*

5ª letra
H *conductores apantallados independientes*
K *funda de PVC*
L *funda de PE*
N *funda de PA*
P *pares con funda independiente*

4ª y 5ª letras
C *cable con refuerzo embutido en la funda*
E *diseño reforzado*
J *cable para enterrado o armadura de fleje de acero con cubierta metálica*
R *cable de control o de señales*
X *línea PSTN*
Y *línea PSTN resistente a las inclemencias del tiempo*

Transmisión de datos por fibra óptica



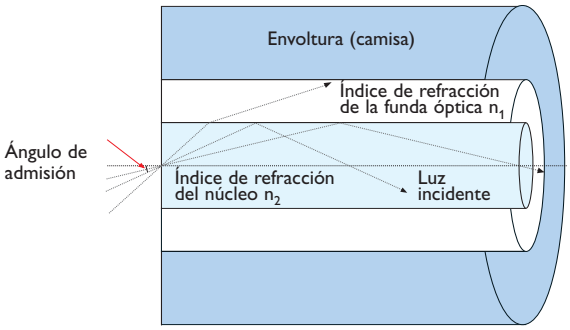
La principal ventaja del cable de fibra es que es totalmente inmune a las perturbaciones eléctricas y magnéticas. Por este motivo, es la solución ideal para los entornos industriales difíciles. Garantiza una transmisión fiable y ofrece una elevada capacidad de transmisión de datos. El cable de fibra se puede utilizar en determinadas secciones sensibles de la red y se puede combinar en el sistema utilizando un módem con, por ejemplo, cable de 4 hilos. La inversión que requiere la instalación de una red de fibra óptica es todavía ligeramente más costosa que la de hilo de cobre, pero ofrece muchas ventajas. Además, como el mercado está creciendo, los precios son cada vez más bajos.

La gama de productos de fibra de Westermo transforma las señales eléctricas en pulsos de luz que a continuación se envían por el cable a través de un transmisor de fibra óptica equipado con un diodo electroluminiscente o láser. El diodo láser permite transmitir a mayor distancia y a velocidades más elevadas, pero resulta más caro, razón por la cual está más extendido el uso de diodos electroluminiscentes. El receptor alberga un fotodiodo que vuelve a transformar los pulsos de luz en señales eléctricas.

Cable de fibra óptica

En principio, el vidrio del cable de fibra puede ser de dos tipos, con distinto índice de refracción. La fibra está formada por el núcleo, que es la parte central y la funda óptica, que es la parte que rodea al núcleo.

Al entrar en la fibra, el pulso de luz se refleja por el cable debido a que la frontera entre las dos capas actúa como un espejo (a condición de que la luz entrante no incida en un ángulo demasiado grande).



El núcleo y la funda óptica del cable de fibra están recubiertos por una envoltura exterior cuya única función es proteger la fibra de las influencias externas.

La elección del cable depende de requisitos como los siguientes:

- Material
- Cable monomodo o multimodo
- Índice gradual o en escalón
- Longitud de onda del transmisor

Material

El material que se utiliza para el núcleo y la funda varía de un tipo de fibra óptica a otro. El más común es el vidrio, constituido de dióxido de silicio extremadamente puro. No obstante, también hay fibra silicoplástica (PCS, Plastic-Clad Silica) en la que el núcleo es de vidrio y la funda de plástico, y también cables en los que tanto el núcleo como la funda son de plástico.

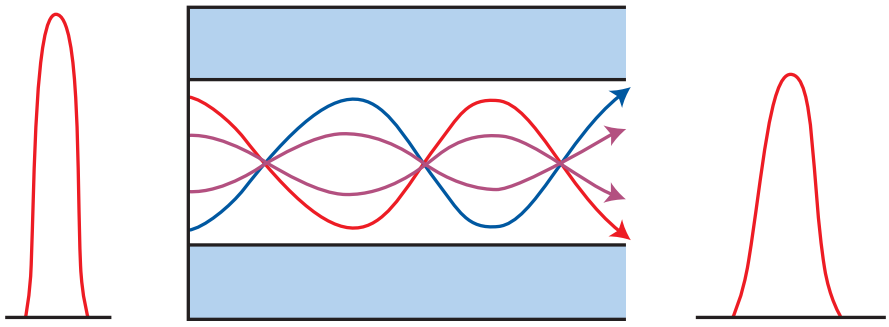
El de mejor rendimiento es el de fibra de vidrio, aunque sus terminaciones son más complicadas. En cambio, la fibra de plástico tiene unas terminaciones más sencillas, pero su rendimiento es el más bajo de todos.

Atenuación en la fibra multimodo

Dependiendo del grosor del material del núcleo, el cable puede ser de dos tipos: multimodo o monomodo.

El cable multimodo más corriente tiene un núcleo de 62,5 µm y una funda de 125µm (de ahí su designación: 62,5/125).

El cable monomodo más corriente tiene un núcleo de 9 µm y una funda de 125 µm (9/125).



Pulso de luz transmitido | **Trayectoria de la luz en cable multimodo de índice gradual** | **Pulso de luz recibido**

Multimodo

El núcleo del cable multimodo es lo suficientemente grande para permitir varios modos. Este tipo de cable puede ser además de índice gradual o de índice en escalón. En la fibra de índice en escalón, algunos de los modos que se reflejan por el cable tienen que viajar más lejos que otros; al hacerlo, el pulso de luz se propaga. Como resultado, el ancho de banda es menor, lo que constituye un inconveniente. El cable de índice gradual resuelve este problema. En este tipo de cable, el índice de refracción disminuye paulatinamente desde el centro del núcleo hacia la funda, de tal modo que el haz de luz que va por el centro del cable circula con más lentitud que los que van por la parte exterior, lo que mantiene el pulso unido.

Atenuación en la fibra monomodo

El núcleo del cable monomodo es tan fino que sólo tiene capacidad para un modo, lo que significa que el pulso de luz transmitido no se distorsiona a su paso por el cable.

Longitud de onda

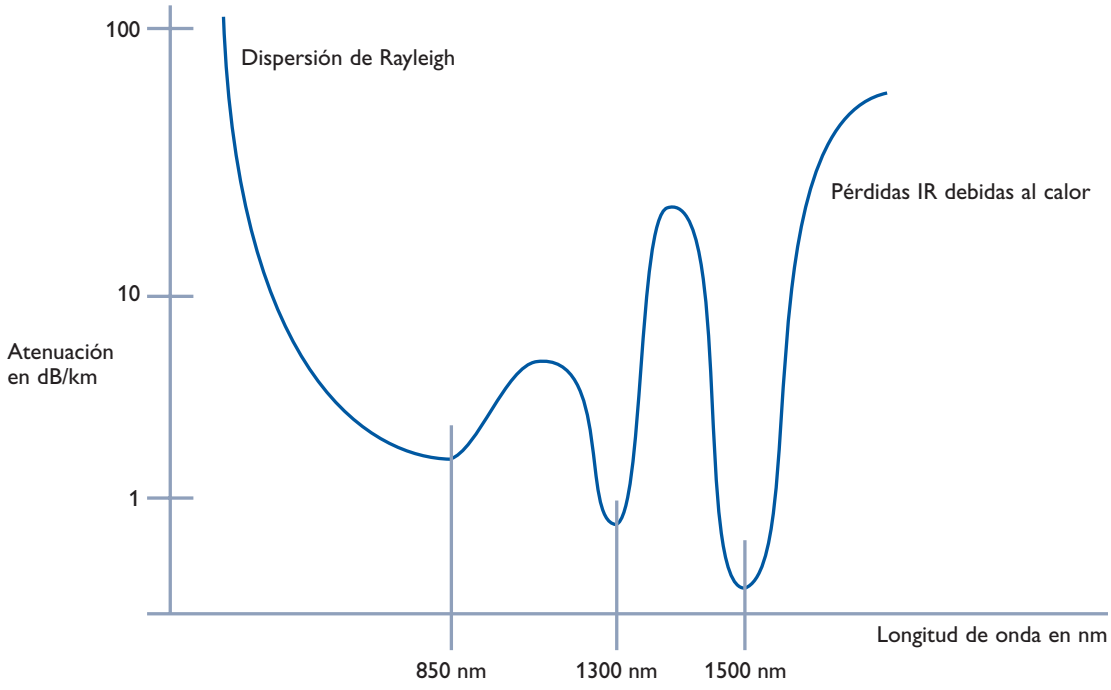
Pulso de luz transmitido

Trayectoria de la luz en cable monomodo

Pulso de luz recibido

La atenuación del cable también depende de la longitud de onda de la luz emitida por el transmisor. Las longitudes de onda que presentan valores de atenuación bajos son 820 nm, 1300 nm y 1550 nm. El cable monomodo solamente propaga con eficacia las frecuencias más elevadas.

Atenuación de la luz en cable de fibra de vidrio a diferentes longitudes de onda

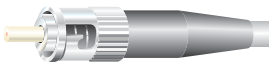


Resumen de los tipos de fibra

Material	Tipo	Núcleo/Funda	Atenuación (dB/km)	Campo de aplicación
Plástico	Multimodo Índice en escalón	200-600/450-1000 um	330-1000	Instalación sencilla Distancias cortas
Núcleo de vidrio (silicio) y plástico	Multimodo Índice en escalón	200-600/350-900 um	4-15	Bajo coste, Distancias cortas
Vidrio	Multimodo Índice en escalón	50-400/125-440 um	4-15	Bajo coste, Distancias cortas
Vidrio	Multimodo Índice gradual	30-100/100-140 um	2-10	Coste intermedio Distancias medias
Vidrio	Monomodo	3-10/50-125 um	0,4-5	Coste elevado Distancias largas

Terminaciones

Existen varias maneras de terminar un cable de fibra óptica. La forma más fácil es la del cable multimodo de fibra de vidrio. Uno de los procedimientos más sencillos es el de «engaste y corte», que consiste en insertar el conector en la fibra a presión con unos alicates especiales y luego cortar la fibra con cuidado. Otro procedimiento de montaje, más seguro que el anterior, es el de encolar el conector a la fibra con resina epoxi (algunos conectores ya llevan el adhesivo). El conector se calienta en un horno especial durante un minuto aproximadamente, luego se inserta la fibra y se deja enfriar. Ambos procedimientos requieren herramientas para preparar la fibra antes del montaje del conector y para pulirla una vez terminada la operación. En los sistemas en los que los puntos de conexión cambian a menudo, es recomendable utilizar el segundo procedimiento, ya que proporciona unas terminaciones más duraderas. El mercado ofrece gran variedad de conectores para fibra óptica, pero para las aplicaciones industriales se utilizan básicamente los cuatro tipos siguientes:



ST conector símplex para multimodo, 2 km

MTRJ conector dúplex para multimodo, 2 km, o monomodo, 15/40 km.

SC conector símplex para multimodo, 2 km, o monomodo, 15/40 km.

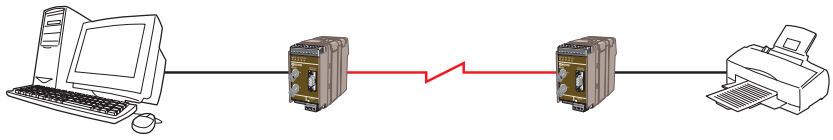
LC conector dúplex para monomodo, 15/40/85 km.

Cálculo del balance de pérdida

La distancia de transmisión de un sistema depende de la potencia de transmisión, la sensibilidad del receptor y las pérdidas por las terminaciones y empalmes del cable. Para calcular esta distancia se elabora un balance de pérdida por la fibra óptica, que refleja en valores típicos y mínimos la diferencia entre la potencia de salida del transmisor y la sensibilidad del receptor. En Westermo hace tiempo que decidimos incluir estos valores en la documentación de casi todos nuestros productos, debido a las grandes diferencias existentes en las especificaciones de los distintos fabricantes, sobre todo en lo que concierne a la fibra monomodo.

Ejemplo

Supongamos que deseamos conectar dos equipos utilizando dos MD-62. ¿Conviene utilizar fibra multimodo o monomodo? El cable multimodo presenta una atenuación de 3,2 dB/km a 820 nm, mientras que en el cable monomodo ésta es de 0,5 dB/km a 1.300 nm. Supongamos que la distancia de transmisión es de 6 km, y que el cable incluye dos empalmes, cada uno de los cuales genera una atenuación de 0,2 dB.



Opción 1, cable multimodo
3,2 dB/km x 6 + 2 x 0,2 dB = 19,6 dB

Opción 2, cable monomodo
0,5 dB/km x 6 + 2 x 0,2 dB = 3,4 dB

Según el manual del MD-62, el balance de fibra mínimo para:
cable multimodo 62,5/125 con una longitud de onda de 820 nm es de: 14,5 dB
cable monomodo 9/125 con una longitud de onda de 1.300 nm es de: 6,3 dB

Por consiguiente, en el caso del ejemplo habría que instalar cable monomodo.
No obstante, este es sólo un ejemplo de la manera en que debe utilizarse el balance de pérdida de la fibra para calcular la distancia de transmisión. En nuestro ejemplo conocemos el balance de pérdida de la fibra porque figura en el manual del MD-62.

Modelo OSI

Para que los sistemas puedan comunicarse entre sí, se requiere un marco estructurado que permita interconectar productos de diferentes proveedores. Este fue el motivo que llevó al desarrollo del modelo OSI (**O**pen **S**ystem **I**nterconnection, esto es, interconexión de sistemas abiertos). Creado por la Organización Internacional de Normalización (más conocida por sus siglas en inglés, ISO), este modelo explica cómo funciona la comunicación entre dos sistemas cualesquiera. El objetivo es, como su propio nombre indica, propiciar el desarrollo de sistemas abiertos y, por consiguiente, independientes del fabricante. Los sistemas propietarios no se pueden comunicar con equipos fabricados por otras empresas, pero el problema se soluciona utilizando un protocolo normalizado. En todo caso, hay que tener en cuenta que el modelo OSI no es un protocolo, y que su finalidad es explicar y diseñar redes flexibles, robustas y, por encima de todo, abiertas.

Estructura del modelo OSI

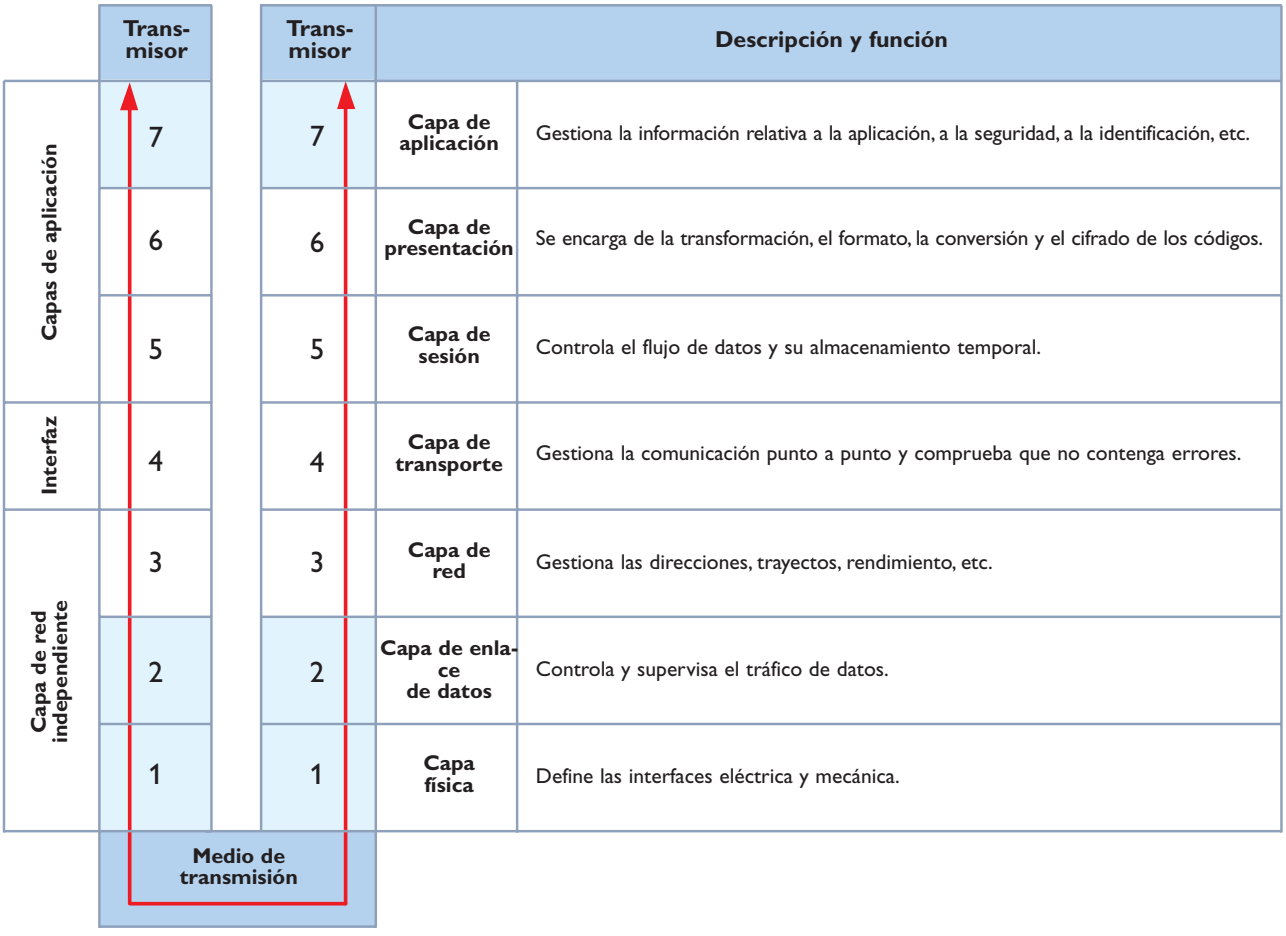
En 1983, la **O**rganización **I**nternacional de **N**ormalización (ISO) creó el modelo OSI (**O**pen **S**ystem **I**nterconnection Modelo de referencia) precisamente con ese fin. El modelo define todas las partes, estructuras y funciones que se necesitan para la comunicación, y las divide en siete capas o niveles en función de las diferentes etapas del proceso de comunicación.

En pocas palabras, se puede decir que cada capa (salvo la de aplicación) funciona de tal manera que siempre se puede comunicar con la capa adyacente. Para hacer posible además la comunicación entre las capas, se amplía la información con la inclusión de una cabecera, algo que resulta imprescindible para que la capa subyacente pueda interpretar y gestionar los datos. Cuando los datos llegan al receptor, cada capa retira la información añadida (la cabecera) que necesita y envía la información a la capa inmediatamente superior. Cuando la información llega a la capa superior, toda la información adicional ha desaparecido. En definitiva, cada capa se comunica con la capa correspondiente del otro ordenador.

En la norma europea V. 24, por ejemplo, se trata de una especificación lógica que viene determinada por la capa física y que sólo define la tarea de las líneas: control, datos y distancias de transmisión posibles. Por eso la norma V.24 se completa con una especificación electrónica conocida como V.28, que también es un subconjunto de la capa física.
V.24 y V.28 tienen su contraparte en la norma americana RS-232, que especifica tanto la interfaz eléctrica como la física.

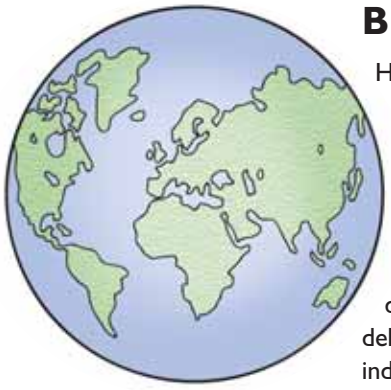
Ejemplo comparativo

Con el fin de ofrecer una imagen más clara del modelo OSI, vamos a hacer una comparación con una llamada de teléfono cualquiera.



- La capa física está formada por la red telefónica y las definiciones de las señales transmitidas.
- El control de enlace lógico (LLC) de la capa de enlace de datos se corresponde con el altavoz y el micrófono del teléfono. El control de acceso a los medios (MAC) de la capa de enlace incluye los componentes del teléfono que transforman las señales del micrófono en señales que el teléfono puede trasmitir por la red y que las devuelven al formato original al llegar al receptor.
- La capa de red se corresponde con la pulsación de las teclas del teléfono.
- La capa de transporte realiza una función similar a que se produce en el teléfono al llamar a otro abonado: al marcar el número, se establece una conexión a través de la capa de transporte que garantiza el contacto con el receptor.
- La capa de sesión se puede comparar con la llamada.
- La capa de presentación tiene su equivalente en la conversación.
- La capa de aplicación coincide con la llamada completa.

Transmisión local de datos



Buses de campo

Hoy en día, cada parte de un sistema moderno de automatización ha de tener capacidad para comunicarse, pero además debe poder hacerlo utilizando vías de comunicación uniformes. Los requisitos de la transmisión de datos aumentan sin cesar, tanto en horizontal (nivel de campo) como en vertical (con el aumento de los niveles jerárquicos). Por lo general, las soluciones de transmisión de datos totalmente integradas para el sector industrial incluyen todos estos elementos. Es algo que se aplica a todo, desde las señales de los sensores, que a su vez están conectados a instrumentos, válvulas, motores, etc. En efecto, estos componentes subyacentes del sistema se comunican con los sistemas de control principales o los ordenadores industriales donde se ejecuta la aplicación.

En este principio se basa el concepto de bus de campo. Pero, ¿qué es en realidad un bus de campo?
En pocas palabras, se podría decir que los buses de campo son algo similar a Internet, pero para la industria. Básicamente permiten interconectar máquinas y otros equipos en una red, de manera que todos los dispositivos se puedan comunicar entre sí y con otros sistemas. Cuando surgió la idea a finales de los ochenta, la fuerza impulsora fue el deseo de acortar los tiempos de instalación y reducir el cableado, es decir, los costes. Este aspecto ha ido perdiendo importancia poco a poco, y actualmente lo que interesa es sobre todo el intercambio de información. Se podría decir que el bus de campo del mañana se parecerá cada vez más a Internet e incluso es posible que se base en la misma tecnología.

Por todo ello, la elaboración y la aceptación de normas internacionales sobre los sistemas de bus de campo es de vital importancia. La norma IEC 61158, que describe los buses de campo, lleva por título «Digital Data communication for measurement and control. Fieldbus for use in industrial control systems» (Transmisión digital de datos para medición y control. Bus de campo para sistemas de control industriales) y está dividida en 6 partes.

Documento IEC 61158	Índice	Capas OSI
61158-1	Introducción	
61158-2	Especificación y definición de los servicios	Capa 1 – Física
61158-3	Definición de servicio	Capa 2 – Enlace de datos
61158-4	Especificación de protocolo	Capa 2 – Enlace de datos
61158-5	Definición de servicio	Capa 7 – Aplicación
61158-6	Especificación de protocolo	Capa 7 – Aplicación

Buses de campo

En las comunicaciones industriales se utiliza toda una serie de medios diferentes, entre los que se cuentan el cable de cobre, la fibra óptica, la transmisión por infrarrojos y las tecnologías de radio. La tecnología de bus de campo se desarrolló con el objetivo de sustituir los sistemas que se utilizaban entonces por soluciones normalizadas. Sin embargo, debido a las distintas necesidades, los diferentes campos de aplicación y las soluciones propietarias de algunos de los fabricantes más importantes, actualmente conviven en el mercado varios sistemas de bus, más o menos abiertos y de distintas características. La tabla que sigue a estas líneas ofrece una comparación de los buses de campo más comunes.

Bus de campo	Desarrollado por	Norma	Topología	Medio	Rango máx.	Método de comunicación
PROFIBUS DP/PA	Siemens	EN 50170/ IEC 1158-2	Bus, estrella, anillo	Par trenzado o fibra	100 m a 12 Mbit/s	Maestro/esclavo Entre pares
INTERBUS-S	Phoenix Contact, Interbus club	DIN 19258 EN 50254	Anillo	Par trenzado o fibra	400 m/ segmento 128 km en total	Maestro/esclavo
DeviceNet	Allen-Bradley ODVA	ISO 11898 ISO 11519	Bus	Par trenzado	500 m (según la velocidad)	Maestro/esclavo Multimaestro Entre pares
LonWorks®	Echelon Corp.		Bus, anillo, bucle, estrella	Par trenzado o fibra	2.000 m @ 78 kbit/s	Maestro/esclavo Entre pares
CAN abierto	CAN In. Automation	CiA	Bus	Par trenzado	25 – 1.000 m (según la) velocidad)	Maestro/esclavo Entre pares Multidifusión Multimaestro
Ethernet	DEC, Intel, Xerox	IEEE 802.3	Bus, estrella,	Par trenzado o fibra	10/100 Base T 100 metros	Entre pares
Modbus Plus	Modicon		Bus	Par trenzado	450 metros por segmento	Entre pares
Modbus RTU/ASCII	Modicon	EN 1434-3 ICE 870-5	Bus	Par trenzado	1.000 metros	Maestro/esclavo
Data Highway Plus (DH+)	Allen-Bradley		Bus	Par trenzado	3.000 m	Multimaestro Entre pares

PROFIBUS

PROFIBUS es un sistema de comunicaciones digital uniforme y abierto adecuado para una amplia variedad de aplicaciones, sobre todo de ingeniería y automatización de procesos. PROFIBUS es ideal tanto para las aplicaciones en las que la rapidez es vital como para las aplicaciones donde la comunicación resulta compleja. La comunicación PROFIBUS se basa en las normas internacionales IEC 61158 e IEC 61784, por lo que satisface las exigencias de los usuarios de buses de campo de disponer de un sistema abierto e independiente del fabricante. En efecto, la comunicación entre productos de distintos fabricantes no requiere ninguna adaptación ni software especializado.

Historia

La historia de PROFIBUS se remonta al año 1987, cuando un grupo de empresas e instituciones europeas elaboró una estrategia para desarrollar un bus de campo. En total, el grupo constaba de 21 miembros, entre empresas, universidades, otras instituciones y diferentes organismos. El objetivo era crear un bus serie que obtuviera la aceptación general. Pero el grupo se fijó además un importante objetivo intermedio: normalizar una interfaz para dispositivos de campo. Con el fin de elaborar una norma general, los miembros participantes de la ZVEI (la asociación central de la industria eléctrica) acordó dar su apoyo a un concepto técnico común para ingeniería y automatización de procesos. El primer paso fue la especificación del complejo protocolo de comunicación PROFIBUS FMS (**F**ieldbus **M**essage **S**pecification), diseñado para aplicaciones de comunicación muy exigentes. El siguiente paso se dio en 1993, cuando se terminó la primera especificación del protocolo Profibus DP, más sencillo y considerablemente más rápido. DP es la abreviatura de **D**ecentralized **P**eripherals. Este protocolo se ha seguido desarrollando a lo largo de los años, y actualmente está disponible en tres versiones, cada una de ellas con un grado distinto de funcionalidad: DP-V0, DP-V1 y DP-V2. Otro protocolo además del DP es el PROFIBUS PA (**P**rocess **A**utomation), desarrollado para los requisitos específicos de la industria de procesos. Motion Control es una versión para equipos motrices, mientras que PROFIsafe es para aplicaciones de seguridad. En este manual únicamente se describen aplicaciones DP.

Comunicación PROFIBUS

Profibus se basa en RS-485, probablemente la técnica de transmisión de datos más común del sector industrial, que utiliza par trenzado apantallado y admite velocidades de transmisión de hasta 12 Mbit/s. Recientemente se ha especificado la versión RS-485-IS, un medio de transmisión de 4 hilos para clase de protección E y uso en entornos explosivos.
La técnica de transmisión MBP (**M**anchester coded, **B**us **P**owered) se utiliza en aplicaciones de automatización de procesos que requieren suministro eléctrico por el bus a unidades en zonas de seguridad intrínseca. En las aplicaciones expuestas a interferencias electromagnéticas se recomienda transferir los datos PROFIBUS por fibra óptica, entre emplazamientos de instalación con potencial de tierra diferente y para cubrir grandes distancias.

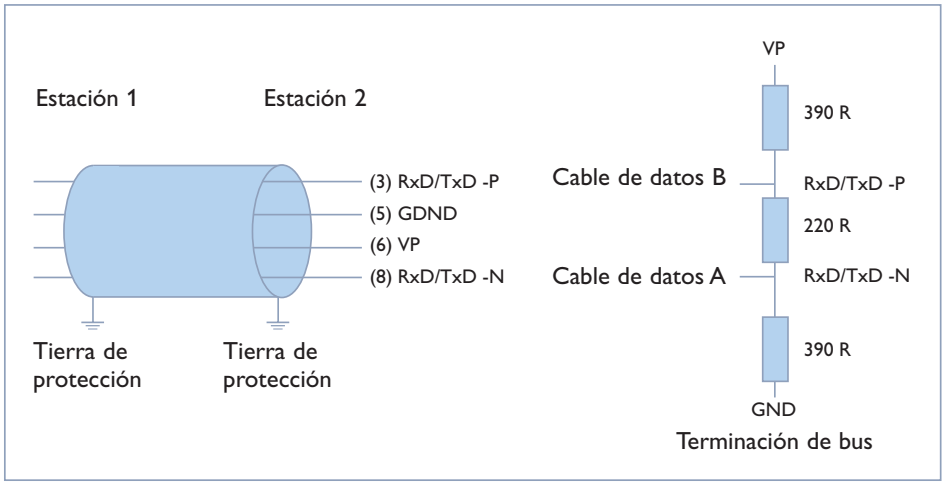
Velocidad de transmisión de datos (kbit/s)	Longitud máx. segmento (m)
9,6	1200
19,2	1200
45,45	1200
93,75	1200
187,5	1000
500	400
1500	200
3000	100
6000	100
12000	100

Valores referidos al **cable de tipo A,** que tiene las características siguientes:

Impedancia característica	135–165 Ω
Capacidad	<30 pf/m
Resistencia de bucle	110 Ω/km
Diámetro del núcleo	0,64 mm
Sección del cable	>0,34 mm^2

Topología de red de PROFIBUS

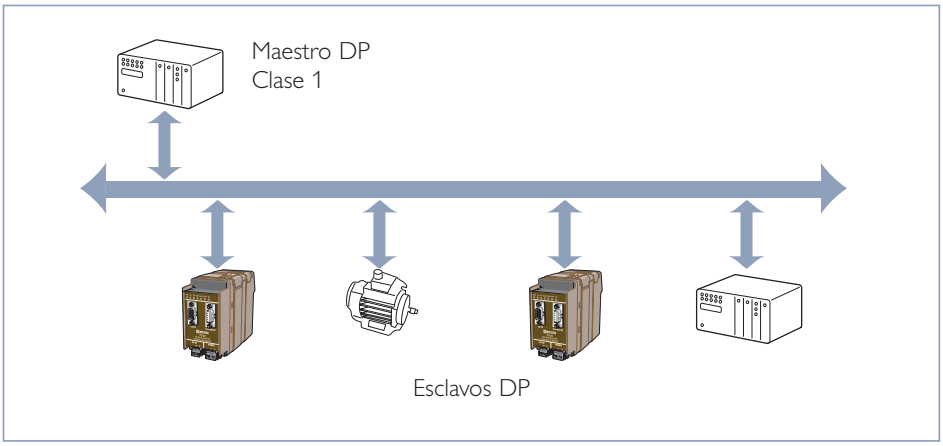
Dado que la interfaz básica es RS-485, los dispositivos deben conectarse en una estructura de bus. Cada segmento admite la conexión de hasta 32 estaciones. En los extremos de cada segmento se conecta una terminación de bus activa (consulte la figura). En efecto, ambas terminaciones deben recibir tensión constantemente para evitar errores de transmisión. La terminación del bus suele ir integrada en los conectores y se activa mediante un switch. Si el número de estaciones conectadas a la red es mayor de 32, o si las distancias de transmisión superan los valores indicados en la página 51, es necesario utilizar un repetidor. No obstante, conviene recordar que el repetidor aumenta la carga eléctrica de la red y que, por consiguiente, aquellos segmentos que cuenten con un repetidor solamente podrán tener conectadas 31 estaciones. Utilizando repetidores regenerativos se pueden interconectar hasta 10 segmentos en línea.



PROFIBUS DP

Representa un intercambio de datos de proceso básicos, rápidos, cíclicos y deterministas entre el maestro y sus esclavos asignados. El maestro, que suele ser un sistema de control programable central (como un PLC o un PC industrial), regula y controla la comunicación con los esclavos.

Maestro y esclavo



Un esclavo es un dispositivo de campo (terminal de E/S, equipo motriz, estación de interfaz hombre-máquina, válvula, transmisor, instrumento de análisis o similar) que lee datos sobre el proceso o utiliza datos de salida para controlar el proceso. También existen unidades que sólo procesan datos de entrada o salida, sin alterar el proceso. Desde el punto de vista de la transmisión, los esclavos son elementos pasivos que sólo responden a peticiones directas.

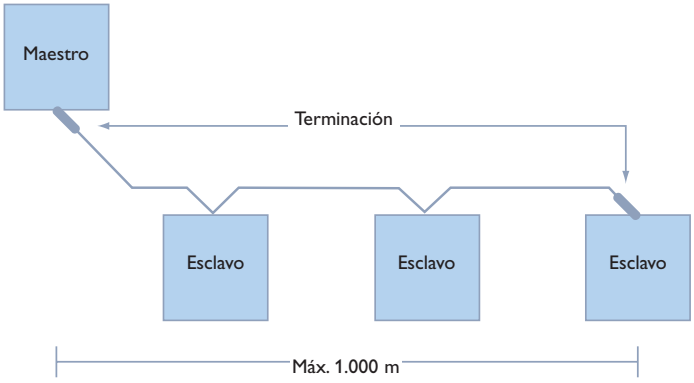
Transmisión cíclica de datos entre DPM1 y los esclavos

La transmisión de datos entre un maestro DP de clase 1 (DPM1) y los esclavos que tiene asignados es totalmente automática, según una secuencia repetida definida. El usuario asigna los esclavos durante la configuración del sistema de bus, al mismo tiempo que determina qué esclavos desea incluir/excluir en la transmisión cíclica.

Modbus

Modbus ASCII y Modbus RTU

Modbus ASCII y Modbus RTU son protocolos que se han convertido en una norma de facto en numerosas aplicaciones. Desarrollado por Modicon a principios de la década de 1970, Modbus se basa en una red multipunto integrada por un maestro y varios esclavos. Modbus no se diseñó exclusivamente para aplicaciones industriales, sino que se puede utilizar siempre que exista la necesidad de controlar un proceso o el flujo de información.



Los dispositivos conectados a Modbus ASCII y Modbus RTU utilizan para la transmisión de datos la interfaz serie RS-232 o la RS-485. La principal diferencia entre ellos es que en Modbus RTU cada byte de 8 bits del mensaje contiene dos caracteres hexadecimales de 4 bits, mientras que en Modbus ASCII cada byte de 8 bits del mensaje se envía como dos caracteres ASCII. RTU es, por tanto, más eficaz y tiene capacidad para transmitir más datos, pero si un paquete de datos se rompe durante la transmisión, es incapaz de recomponerlo. En cambio, Modbus ASCII sí admite espacios en la transmisión, lo que ha hecho de este protocolo el preferido para la transmisión de datos por módem.

La velocidad de transmisión máxima suele estar limitada a 19,2 kbit/s. La comunicación, controlada por un maestro, sólo puede ser en modo half dúplex, y los esclavos no se pueden comunicar entre sí.

El protocolo Modbus básico entre un maestro y un esclavo incluye los elementos siguientes:

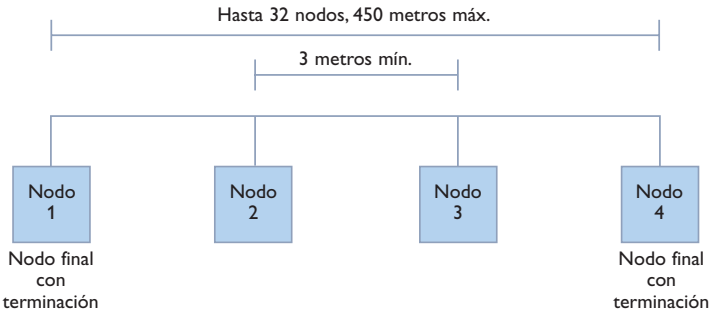
Dirección	Código de función	Datos	Corrección de errores

Modbus Plus

Modbus Plus es un tipo de red para aplicaciones industriales basado en el intercambio de testigos y la comunicación entre pares o entidades iguales. El intercambio de testigos y la comunicación entre pares requiere una estructura lógica en anillo, en la que todos los nodos puedan iniciar la comunicación pero en la que ninguno de ellos pueda hacerlo hasta disponer del testigo. La velocidad de transmisión es de 1 Mbit/s con par trenzado apantallado. Modbus Plus es una red abierta para el intercambio de información entre los nodos de una red que permite controlar y supervisar procesos industriales.

Además, la red es totalmente transparente, lo que significa que se puede llegar a cualquier dispositivo del sistema a través del punto de conexión.

La interfaz se basa en la norma RS-485 y está formada por secciones que admiten la conexión de hasta 64 nodos. Cada segmento de cable admite una distancia de transmisión de 450 metros y permite conectar directamente 32 nodos. No obstante, si la distancia de transmisión es mayor o hay que conectar más de 32 nodos a un segmento, se puede utilizar un repetidor. Cada sección puede ser de 1.800 metros como máximo, pero se pueden cubrir distancias mayores utilizando un módem de fibra óptica.

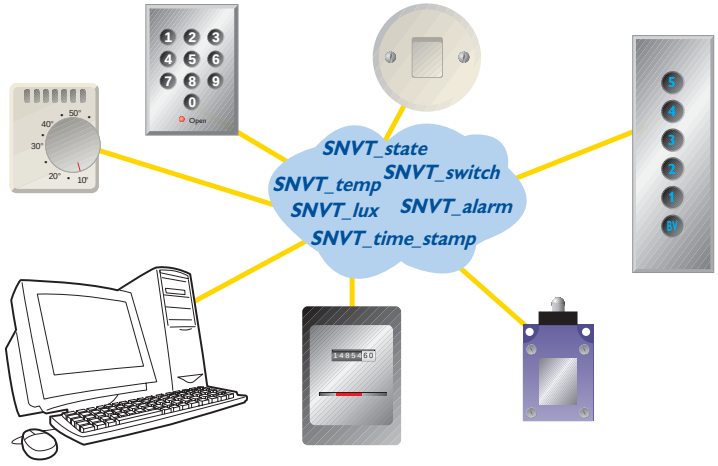


MODBUS/TCP

Modbus/TCP es una variante de Modbus, un protocolo de comunicación abierto para control y supervisión de equipos de automatización. Este protocolo combina las propiedades de Modbus con el protocolo TCP/IP, que permite el intercambio de datos dentro de la intranet o a través de Internet. Utilizando un servidor serie se puede encapsular un paquete Modbus ASCII o Modbus RTU en un paquete TCP o UDP, aunque conviene recordar que el resultado no es un paquete Modbus/TCP. En Modbus TCP, cada nodo conoce su dirección IP y se comunica con TCP por el puerto 502.

LON®WORKS

Con la introducción de la tecnología LONWORKS®, Echelon® Corporation creó una plataforma completa sobre la cual desarrollar sistemas de control distribuidos y abiertos, basados en una arquitectura de red inteligente. Por lo general, el sistema LONWORKS® está formado por varios dispositivos inteligentes (llamados nodos), cada uno de los cuales realiza una tarea específica, por ejemplo, medir la temperatura o controlar una válvula. Los nodos intercambian información básica por la red. Las redes que se utilizan para control y se basan en esta estructura de inteligencia distribuida se conocen como redes de arquitectura entre pares. Normalmente los nodos no se envían comandos, sino que intercambian paquetes de datos que contienen información sobre, por ejemplo, temperatura, presión,



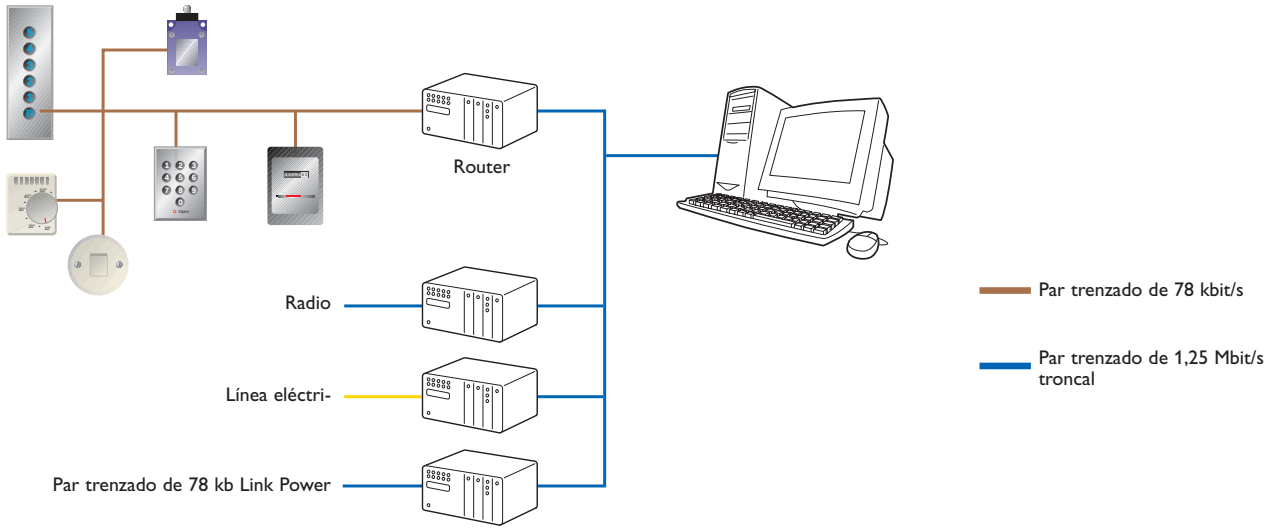
LONWORKS®: una red orientada a datos

estado, fecha y hora. A continuación, cada nodo utiliza la información recibida de distinta manera, dependiendo de la función específica que tenga asignada. En LONWORKS®, los paquetes de datos se interpretan como variables globales disponibles en la red, motivo por el cual se los denomina «variables de red». Cuando un nodo actualiza una variable de red, ésta se envía automáticamente a la red, para que los demás nodos tengan acceso al nuevo valor. Dentro de la tecnología LONWORKS®, la interoperabilidad es clave. Una de las condiciones de la interoperabilidad es que los nodos de distintos fabricantes puedan intercambiar y comprender los datos sin ninguna modificación especial del software o el hardware. Para que esto sea posible, no basta con que los nodos estén en la misma red, tengan el mismo transceptor y sean capaces de enviar variables de red. Además deben comprender el contenido de las variables de red. Por ejemplo, los nodos deben saber si la

temperatura viene expresada en grados Fahrenheit o en grados Celsius, o si un caudal viene indicado en litros/segundo o en mililitros/segundo. Por eso es necesario disponer de normas que regulen la manera en que deben interpretarse los paquetes de datos. En LonWorks®, la normalización está a cargo de una organización llamada «LonMark® Association». Se trata de una asociación independiente integrada por fabricantes de nodos LonWorks®, integradores de sistemas y usuarios finales, que han recopilado una lista de tipos de variables de red normalizadas a la que han denominado SNVT (pronunciado snivit) y que constituyen la abreviatura de «**S**tandard **N**etwork **V**ariable **T**ypes». Estas variables contienen información sobre el dispositivo, la resolución y los valores que puede tomar cada tipo. Por ejemplo, cuando se utiliza el tipo SNVT_speed, todos los nodos LonWorks® saben que la unidad es el metro/segundo, que la resolución es de 0,1 metros/segundo y que los valores admisibles son los comprendidos entre 0 y 6.553,5 metros/segundo.

El transceptor más utilizado es el FTT-10A de topología libre, que se comunica a una velocidad de 78 kbit/s por cable de par trenzado. La expresión topología libre significa que se puede utilizar en redes en estrella, en anillo, en bus o en una combinación de todas ellas. Echelon® también dispone de un transceptor de topología libre denominado LPT-10 LinkPower, que es compatible, en lo que respecta a las señales, con el modelo FTT-10A y que se puede utilizar con él. Lo que hace especial al LPT-10 es que es un «2 hilos verdadero», en el sentido de que el hilo conduce tanto datos como tensión de alimentación. La ventaja de poder mezclar libremente las topologías hace que estos transceptores sean extremadamente útiles en las redes de control actuales, ya que permiten conectar fácilmente dispositivos nuevos. Otra de las ventajas que presentan estos transceptores es que su conexión es insensible a la polaridad, lo que facilita su instalación y elimina el riesgo de realizar conexiones incorrectas. Echelon® tiene además otros transceptores, como el de par trenzado de 1.250 kbit/s para topologías de bus, así como un transceptor para comunicación por la red eléctrica. Gracias a su capacidad de pasar de una banda de frecuencia a otra, de tratar señales avanzadas y de corregir errores, el transceptor de red eléctrica puede contrarrestar con facilidad las perturbaciones procedentes de motores, reguladores, ordenadores y televisores.

El transceptor PLT-22 se puede configurar para comunicaciones por la red eléctrica en la banda de frecuencias pública Cenelec-C o en la banda de frecuencias Cenelec-A, reservada a las compañías eléctricas. Por lo general, la banda C se utiliza para aplicaciones de domótica, así como para aplicaciones comerciales, mientras que la banda A se suele utilizar para la lectura de los contadores de electricidad. Además existen transceptores de terceros para comunicaciones por fibra óptica, radio e infrarrojos. Las redes LonWorks® suelen incluir una combinación de medios diferentes. Para este tipo de redes, Echelon® dispone de routers capaces de transmitir datos LonTalk® entre los distintos medios de diferentes maneras. Es bastante común que los canales equipados con un medio lento estén conec-



tados a una red troncal dotada de un medio más rápido. Como resultado, se produce una segmentación física y lógica de la red que mejora el rendimiento y la seguridad.

Consideraciones sobre las redes LonTalk® grandes

Aumentar las distancias de transmisión entre dos o más segmentos TP/FT utilizando cable de fibra óptica provoca un ligero retraso en la comunicación entre los diferentes segmentos. Como resultado, pueden producirse colisiones, que a su vez ocasionan retransmisiones de los paquetes de datos, con el consiguiente deterioro del rendimiento de la red. Por consiguiente, es aconsejable que la fibra no supere los 25 km. De conformidad con la norma EIA-709.3, está permitido un retraso máximo de 36 ms, lo que debería ser equivalente a una distancia de 6,8 km. Nosotros recomendamos utilizar nuestro router LR-11 para poder transmitir con seguridad datos a distancias mayores, así como por redes de varios segmentos o con más nodos, a 1.250 kbit/s. No obstante, también aconsejamos analizar la comunicación por la red con el analizador de protocolos LonWorks®.

Conexiones remotas

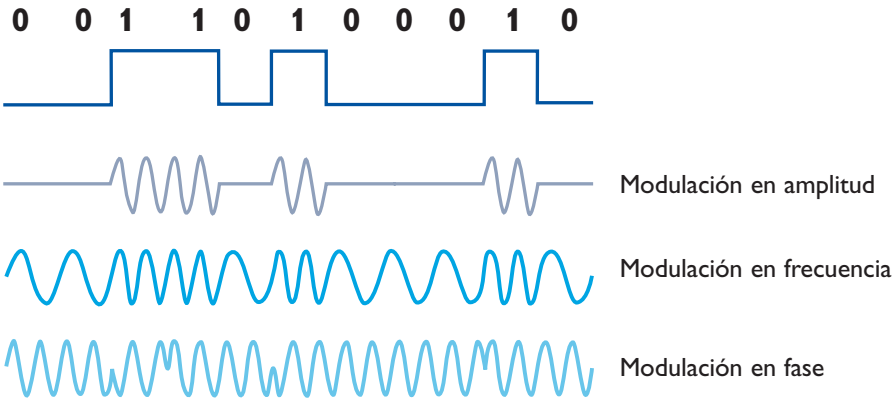
Líneas conmutadas PSTN

Transmisión de datos por la red de telefonía fija

La transmisión de datos a distancia constituye un complemento básico de la transmisión de datos local, pues ofrece la posibilidad de conectarse a fuentes de datos remotas para buscar información sobre, por ejemplo, los mercados, la cotización de las acciones o los registros públicos. El volumen de fuentes de datos disponibles ha aumentado significativamente, y muchas de ellas están conectadas a través de las redes globales. De este modo, es fácil conectarse a una fuente de información financiera en un país y acabar en otra, por ejemplo en Nueva York. Las razones para establecer comunicaciones remotas son muchas (por ejemplo, conectarse por la red telefónica al ordenador de la oficina desde cualquier lugar), y además hoy día resulta muy sencillo, pues muchos ordenadores portátiles tienen integradas las funciones de módem, teléfono móvil y fax.

Conexión por línea conmutada

Las comunicaciones remotas por la red telefónica se basan en el principio de llamar al módem del receptor, esperar a que conteste y establecer una portadora por la línea telefónica. La portadora es la señal que espera el módem. Una vez que cada módem puede escuchar la portadora del otro, se sincronizan con ella. Las velocidades de transmisión por la red telefónica han aumentado mucho en los últimos años, y actualmente no es difícil que alcancen entre 2.400 y 56.000 bit/s. La velocidad de transmisión no sólo depende del módem, sino también de la línea telefónica. En efecto, la distancia y el número de centrales y relés reducen significativamente la calidad de la línea. Por este motivo, muchos módems de alta velocidad tienen capacidad para limitar ésta automáticamente con el fin de garantizar la calidad de la transmisión. Dado que los módems transmisor y receptor a menudo son de distinto fabricante, es fundamental que este tipo de comunicación se ajuste a normas. En la tabla de la página 69 se presentan las velocidades binarias asociadas a diferentes normas.



Modulación

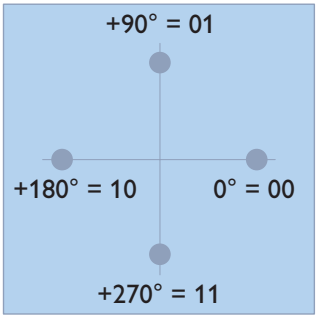
El término módem deriva de las palabras **mo**dulación, es decir, conversión de la señal, y **dem**odulación, esto es, regeneración de la señal original. Para poder transmitir los datos por diferentes tipos de cables, es necesario convertir y adaptar las señales. Los niveles de señal digital (unos y ceros) se convierten en transformaciones que el cable correspondiente puede interpretar. Existen tres tipos básicos de modulación: la modulación en frecuencia, en la que se utilizan distintos valores de frecuencia para representar los ceros y unos; la modulación en fase, que utiliza la variación de fase de la portadora para representar los ceros y unos; y la modulación en amplitud, que utiliza niveles de señal, o picos de amplitud, para generar unos y ceros interpretables. Combinando estos tres tipos básicos se pueden crear técnicas de modulación más complejas.

¿Es lo mismo un bit por segundo que un baudio?

La velocidad de transmisión de un módem telefónico se describe tanto en términos de bit/s (velocidad binaria) como de baudios (velocidad de modulación). La confusión resultante hace necesario explicar un poco estos conceptos.

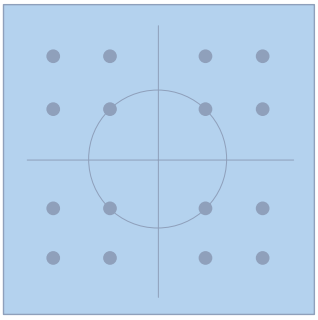
Velocidad binaria: Número de bits que se envían por segundo a través de la interfaz serie. Se mide en bit/s

Velocidad de modulación: Número de combinaciones de señales que se envían por segundo a través de la interfaz de línea. Se mide en baudios



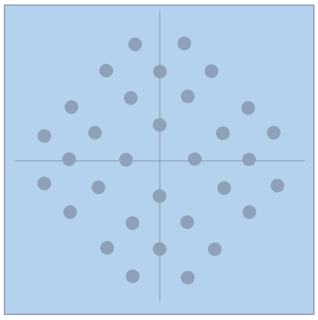
Para aumentar la velocidad de transmisión en un módem telefónico, se modulan juntos más bits y se transmiten a través de la red telefónica. En el ejemplo se muestra la técnica de modulación en fase, en la que se describen dos bits por variación de fase de la señal de línea (V.22).

En este ejemplo, la velocidad binaria es de 1.200 bit/s, y la velocidad de modulación, de 600 baudios.



Cuando se modulan juntas más señales, se alcanza una velocidad de transmisión mayor. En algunas normas, por ejemplo en V.22 bis, la amplitud y la modulación en fase se combinan en lo que se conoce como QAM (**Q**uadrature **A**mplitude **M**odulation, es decir, modulación por amplitud en cuadratura), y se transmiten 4 bits en cada modulación.

En este ejemplo, la velocidad binaria es de 2.400 bit/s, y la velocidad de modulación, de 600 baudios.



En normas como la V.32, la línea se modula mediante una técnica denominada TCM (**T**rellis **C**ode **M**odulation, es decir, modulación con código reticular), que se corresponde con la modulación QAM pero en la que se incluye un bit adicional para corrección de errores. La razón de ser de este bit adicional es que la frontera entre las combinaciones de bits transferidos se reduce, y se hace necesaria una mayor corrección de errores.

En este ejemplo, la velocidad binaria es de 9.600 bit/s, y la velocidad de modulación, de 2.400 baudios.

Algunas normas

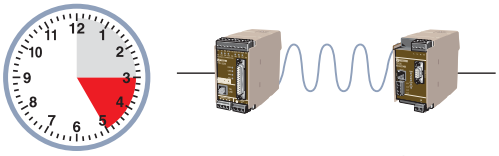
Norma	Vel. binaria	Half/Full	Vel. modulación	Número de bits	Modulación
V.21	300 bit/s	FDX	300 baudios	1 bit/baudio	FSK
V.22	1.200 bit/s	FDX	600 baudios	2 bits/baudio	DPSK
V.22 bis	2.400 bit/s	FDX	600 baudios	4 bits/baudio	QAM
V.23	1.200 bit/s	FDX	1.200 baudios	1 bit/baudio	FSK
V.32	9.600 bit/s	FDX	2.400 baudios	4 bits/baudio	TCM
V.32 bis	14.400 bit/s	FDX	2.400 baudios	7 bits/baudio	TCM
V.34	Hasta 33.600 bit/s	FDX	Hasta 3.429 baudios	*)	TCM
V.90	Hasta	FDX	Hasta	*)	MIC

*) La velocidad de símbolos se negocia durante la sincronización

V.90

V.90 es una norma de módem muy interesante por su potencial para ofrecer velocidades de transmisión elevadas. Para ello, emplea una norma MIC de comunicación parcialmente digital (**M**odulación por **I**mpulsos **C**odificados). Se trata de una norma desarrollada especialmente para la conexión a Internet, por lo que no es simétrica. En efecto, aunque en circunstancias óptimas se pueden alcanzar velocidades de descarga de 56,0 kbit/s, la velocidad de subida es de sólo 9.600 bit/s. Esta norma tiene además el inconveniente de que los proveedores de servicios de Internet tienen que utilizar módems especiales para poder conectar un módem V.90, lo que significa que dos módems V.90 interconectados en realidad no se conectan mediante V.90, sino que lo hacen a través de V.34 bis, ofreciendo así una conexión de 33,6 kbit/s en ambas direcciones.

Conexión



Cuando se establece una conexión de módem, se produce una sincronización en la que se negocian la velocidad de transmisión de datos y el nivel de corrección de errores. La especificación que aparece más abajo muestra los tiempos de conexión entre dos módems con distintas configuraciones de protocolo. Esta medición demuestra que la velocidad de transmisión de datos más rápida no siempre es la mejor. En efecto, el tiempo de conexión es el factor clave cuando lo que hace falta es llamar a varios dispositivos y transmitir un volumen reducido de datos.

Protocolo conexión	Tiempo de
V.32 bis (corrección de errores)	16 s
V.32 bis	13 s
V.22 bis (corrección de errores)	12 s
V.22 bis	7 s
V.23	6 s
V.21	7 s

Lenguaje de los módems telefónicos

Para configurar una conexión, un terminal o un ordenador con software de comunicaciones que utilice el puerto serie del ordenador es necesario establecer comunicación con el módem. Para controlar el módem telefónico se necesitan instrucciones. Con este fin, Hayes Microcomputer Products desarrolló un conjunto de comandos que se ha convertido en un estándar del sector y que se conoce como comandos Hayes®. Se trata de un conjunto de comandos para módem telefónico que sirve para proporcionarle los diferentes parámetros que necesita y que puede enviarse de manera manual desde un ordenador mediante el teclado o de manera automática desde un dispositivo conectado.

Corrección de errores y compresión

La mayoría de los módems telefónicos transmiten datos de manera síncrona, aunque la comunicación entre el ordenador y el puerto serie sea asíncrona, lo que facilita la compresión de los datos. Para controlar la fiabilidad, los datos se pueden dividir en bloques, a cada uno de los cuales se le asigna una suma de comprobación (checksum). Si la transmisión de datos se ve perturbada y la suma de comprobación no es correcta, el receptor solicita el reenvío del bloque. Es lo que se conoce como ARQ (**A**utomatic **R**epeat re**Q**uest, esto es, petición automática de repetición), y el método más común para ello es, según la ITU-T, la corrección de errores V.42, compatible con el protocolo MNP (**M**icrocom **N**etworking **P**rotocol, protocolo de redes de Microcom) y con el procedimiento LAPM (**L**ink **A**ccess **P**rocedure for **M**odems, procedimiento de acceso al enlace para módems).

ARQ y MNP

MNP Nivel 1:
protocolo asíncrono, half dúplex

MNP Nivel 2:
protocolo asíncrono, full dúplex. Los datos se dividen en bloques. La velocidad de transmisión real es algo menor de lo normal.

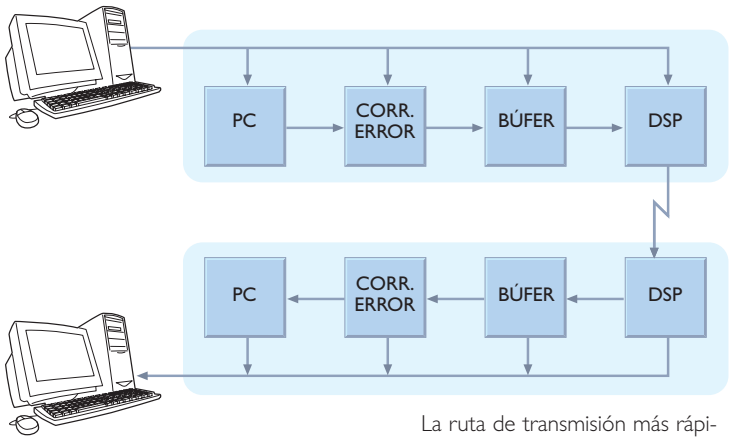
MNP Nivel 3:
protocolo síncrono, full dúplex. Los datos se dividen en bloques. La velocidad es un 10% mayor, con transmisiones sin errores.

Búsqueda y transferencia de archivos

El módem telefónico permite conectarse a otros ordenadores, directa o indirectamente, a través de una red. En un corto espacio de tiempo, Internet se ha expandido y se ha convertido en la red mundial más grande, con 250 millones de usuarios. Mediante el protocolo TCP/IP de Internet es posible enviar correos electrónicos, participar en grupos de discusión, navegar por la red (bases de datos, información y marketing), descargar y subir archivos, hablar por teléfono, celebrar videoconferencias, participar en chats, etc. Sin embargo, existen también otras redes y servicios a los que se accede con módems, como MEMO, Lotus Notes, Compuserve, etc. El módem telefónico permite además trabajar desde casa y conectarse a los ordenadores de la empresa desde un móvil GSM.

Las autopistas del futuro

Actualmente se están dedicando grandes esfuerzos a la elaboración de normas internacionales que regulen la expansión de lo que ya se conoce como las autopistas de comunicaciones del futuro. Las rápidas redes digitales de alta velocidad, como la banda ancha, pueden transmitir grandes cantidades de información (datos, audio y vídeo) por todos los continentes, y la elevada capacidad de la red de televisión por cable puede convertirse en un nuevo recurso que aumente aún más la velocidad de transmisión de datos. Estamos convencidos de que una autopista eficaz ha de comenzar en la propia casa, con una transmisión de datos local de alto rendimiento. En efecto, sobre la base de esta infraestructura esencial se pueden crear rutas de acceso a las redes nacionales e internacionales.



La ruta de transmisión más rápida es siempre la que se conoce como modo directo. Cada etapa de compresión, de corrección de errores y de almacenamiento temporal provoca un retardo.

Línea dedicada

Es un circuito de telecomunicaciones que el operador mantiene siempre conectado y que permite establecer comunicaciones punto a punto o multipunto (V.23) a grandes distancias. Al contrario que en la conexión por línea conmutada, la línea dedicada proporciona un circuito permanentemente establecido entre dos puntos. Esta conexión se puede encaminar por centrales o ser una conexión directa por cable. Lógicamente, los módems telefónicos que incluyen la función de línea dedicada también pueden utilizar cableado estándar para transmitir datos. Se puede establecer una comunicación full dúplex por cable de 2 ó 4 hilos. Los módems de Westermo utilizan varias normas, incluida la V.90, que admite velocidades de transmisión de hasta 56,0 kbit/s. Un módem se configura como emisor y el otro como receptor y, una vez que se ha establecido la conexión, se pueden transferir datos ininterrumpidamente.

MNP Nivel 4:

Los datos se dividen en bloques cuyo tamaño depende de la calidad de la línea. Como son más pequeños que los de Nivel 3, la velocidad de transmisión es un 20% más alta si no hay interferencias.

MNP Nivel 5:

Igual que el Nivel 4, pero con compresión de datos y, por tanto, un aumento de la velocidad que puede ser de hasta el doble.

MNP Nivel 10:

Es una evolución del MNP de Nivel 5 que supervisa la línea de manera dinámica y garantiza una transmisión sin errores.

V.23 sobre línea dedicada

V.23 es una norma antigua diseñada desde el principio para líneas dedicadas. Las velocidades de transmisión de datos están normalizadas a 600 y 1.200 baudios. Los módems que son compatibles con la norma V.23 suelen tener, como mínimo, las siguientes funciones:

- Velocidades de modulación de hasta 600 ó 1.200 baudios.
- Modulación en frecuencia (FSK)

Esta norma utiliza dos modulaciones en frecuencia diferentes:

- Modo 1: 600 baudios a 1.300 Hz–1.700 Hz
- Modo 2: 1.200 baudios a 1.300 Hz–2.100 Hz

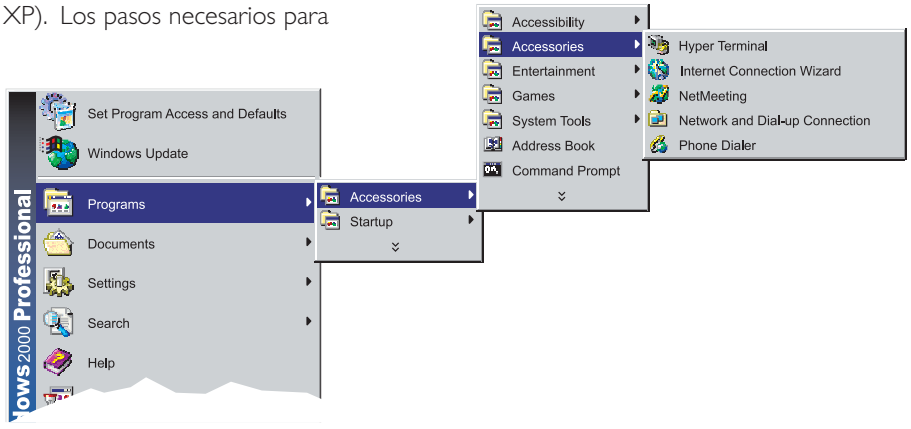
Por lo general, V.23 admite hasta 6 puntos en un cable de 2 hilos. Sin embargo, el número máximo de módems en una línea depende de cómo se hayan instalado los módems, ya que es normal que se produzcan problemas de impedancia. En V.23, la impedancia de línea debe ser de 600 ohmios.

Módem V.23 de Westermo

El módem V.23 de Westermo (TD-23) admite todas las velocidades hasta 1.200 baudios así como terminación con una resistencia de línea de 600 ohmios. Todos los niveles, incluidos los de portadora, transmisión y recepción, son ajustables.

Uso de HyperTerminal

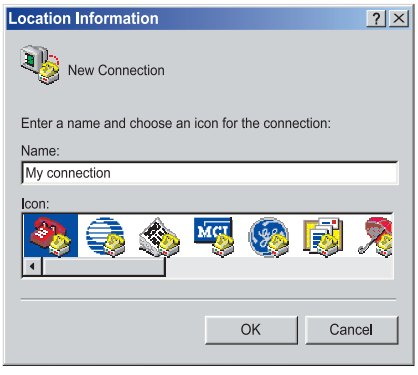
A menudo se requiere un software de emulación serie para poder configurar un módem. Una de las aplicaciones más utilizadas es HyperTerminal para Windows (en este ejemplo se utiliza Windows XP). Los pasos necesarios para utilizar HyperTerminal para comunicarse con un módem son los siguientes:

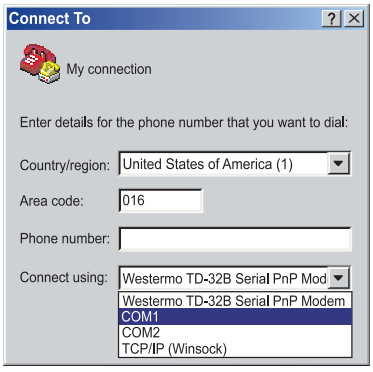


1. Conecte el módem con cable de módem al puerto serie del ordenador (en el ejemplo, Com 1). Como el ordenador es un DTE y el módem es un DCE (consulte la página 26), se utiliza un cable directo con conector de 9 patillas.

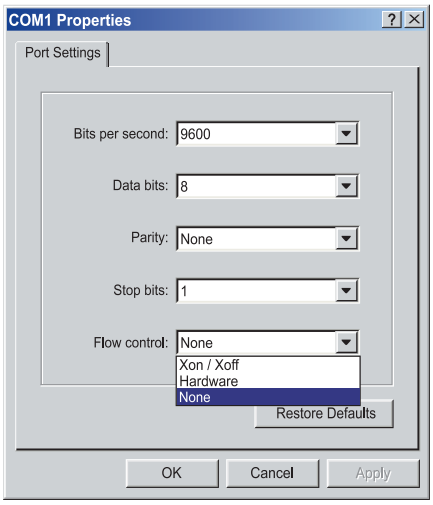
2. Inicie HyperTerminal. La aplicación suele estar en Accesorios/Comunicaciones.

3. Indique un nombre para la conexión, p. ej.: Com 1 9600 8N1 (para Com 19,6 kbit/s 8 bits de datos, sin paridad (N) y 1 bit de parada)





4. Seleccione en la lista desplegable el puerto de comunicaciones que está conectado al módem.
   - Para el ejemplo hemos elegido COM1.
   - Cuando se selecciona COM1, los campos de país o región, código de área y número de teléfono se desactivan.
   - Haga clic en Aceptar.

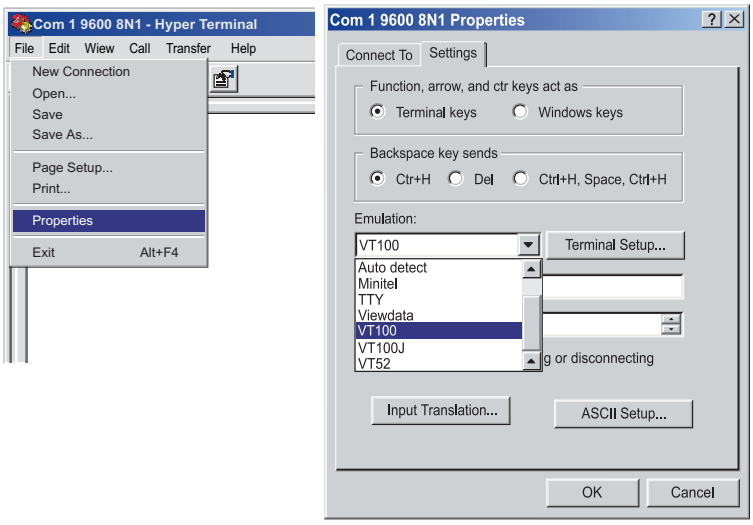


5. Defina las propiedades del puerto: velocidad, bits de datos, paridad, bits de parada y control de flujo. Para el ejemplo, seleccione:
   - Bits por segundo: 9600
   - Bits de datos: 8
   - Paridad: Ninguno
   - Bits de parada 1

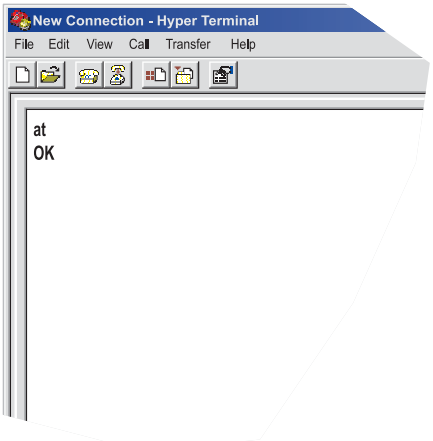
La configuración del control de flujo establece cómo se realiza la sincronización entre el módem y el ordenador.

- Xon/Xoff, significa control por software.
- Hardware, indica señalización con RTS/CTS.
- Ninguno, significa que la sincronización está desactivada.

6. Una vez definidos estos parámetros, HyperTerminal ya está configurado. No obstante, la configuración se puede modificar más adelante desde el menú Archivo, Propiedades, que permite seleccionar, entre otras opciones, la emulación de diferentes terminales, por ejemplo, VT100. El botón Configuración ASCII abre una ventana para definir las condiciones de carácter, avance de línea y eco local.



7. HyperTerminal ya está configurado y listo para usar. Además, como el módem telefónico utiliza comandos AT para la configuración, se puede comprobar si se ha establecido contacto con el módem de la manera siguiente:
   - escribiendo AT y pulsando <intro>
   - El módem debería responder con un OK.

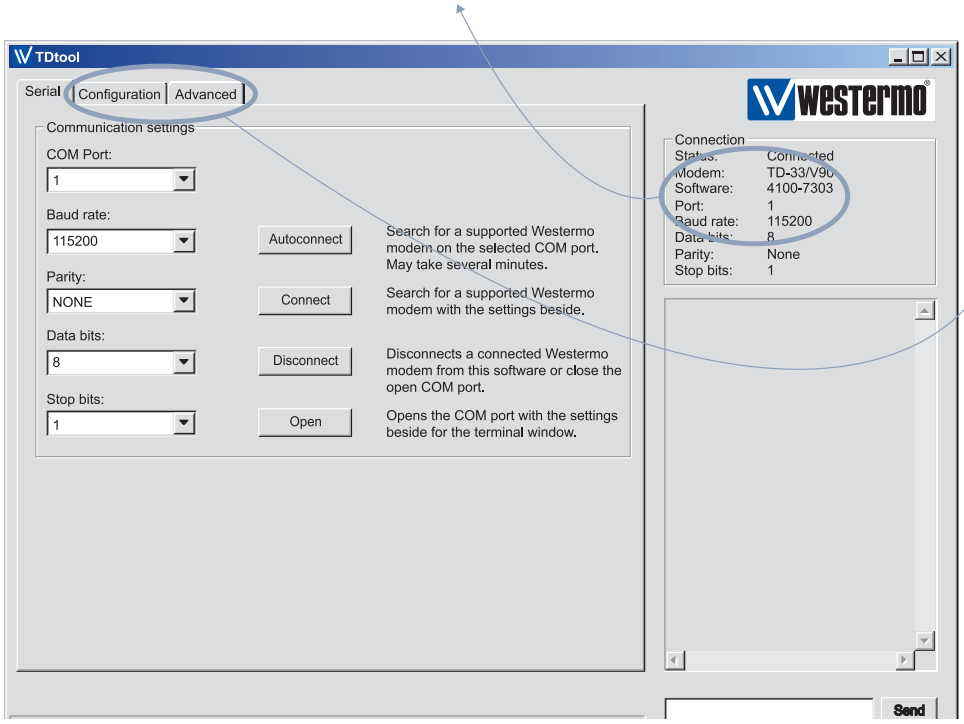


OK es el código que el módem da como resultado para indicar que el comando se ha ejecutado. El comando también configura de manera automática la velocidad, el número de bits, y los bits de paridad y parada del módem.

Una vez establecida la conexión entre HyperTerminal y el módem, se puede configurar el módem. También es importante tener en cuenta las propiedades que utilizará el módem para comunicarse con la aplicación final.

TDtool

Una opción de configuración para nuestros módems es la utilidad TDtool, una aplicación que detecta automáticamente qué módem está conectado y facilita su configuración.



La aplicación detecta los parámetros de configuración del módem conectado. Se aplica a la configuración actual y a las posibles opciones de configuración. Estas opciones se encuentran en las pestañas Configuración y Avanzadas.

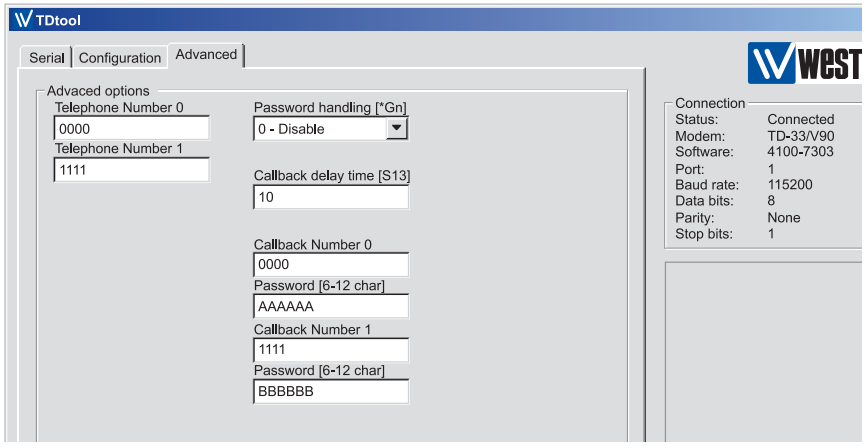
La aplicación TDtool está disponible en nuestro sitio web.

En los ejemplos hemos conectado la aplicación TDtool a dos módems alternativos; las capturas de pantalla muestran cómo se adapta la aplicación en función del módem que esté conectado en cada caso.

Opción 1) Módem TD-33

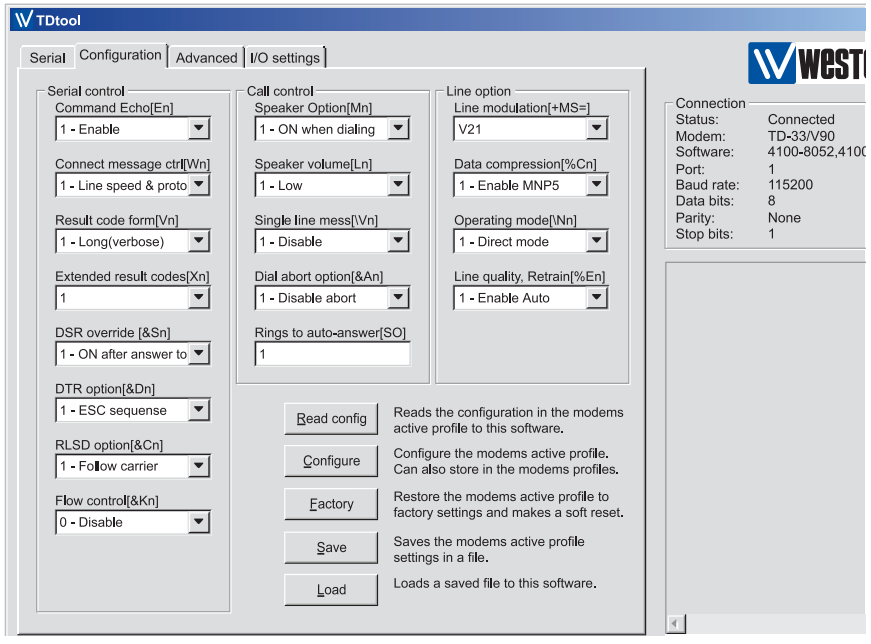
Opción 2) Módem TD-34, un módem que, entre otras características, puede enviar mensajes SMS.

En la pestaña Avanzadas del TD-33 puede escribir el número de teléfono que desea utilizar para la función de call-back (devolver llamada) y la contraseña.



Opción 1 TD-33

En la pestaña Avanzadas del TD-34 hay otras opciones de configuración con las que se pueden ajustar los parámetros SMS necesarios, etc.



Opción 2 TD-34

La aplicación TDtool es un excelente complemento a utilidades como HyperTerminal, debido a que simplifica la configuración de los módems telefónicos. Una vez que se han realizado todos los cambios en la configuración, éstos se descargan en el módem o se guardan en un archivo de texto.

Comandos AT

Los módems telefónicos tienen dos modos de funcionamiento:

- Modo de comandos.
- Modo de comunicación.

En el modo de comandos, se puede configurar el módem para que funcione con la aplicación. El modo de comunicación se utiliza cuando el módem se conecta a otro módem para intercambiar datos.

Como ya hemos mencionado anteriormente, Hayes Microcomputer Products desarrolló un conjunto de comandos que se ha convertido en una norma de facto, conocida como los comandos Hayes®. Estos comandos se utilizan en parte para configurar el módem y en parte para iniciar una conexión.

Debido a que los comandos AT se han convertido en una norma de facto para los módems telefónicos, existen grandes similitudes en la manera en que se utilizan. No obstante, conviene recordar que también existen diferencias, dependiendo de lo avanzado que sea un módem en relación con otro. A continuación se muestran algunos de los comandos más importantes para nuestros módems. Si desea obtener una descripción más detallada de estos comandos, consulte el manual de instalación del módem correspondiente.

ATA – **R**esponder

Fuerza a un módem que se encuentra en modo de comandos a que atienda una llamada entrante. Los módems realizan la sincronización para establecer la conexión. Cuando se establece la conexión, los módems cambian a modo de comunicación.

ATDn – **M**arcar

Hace que un módem que se encuentra en modo comandos inicie una llamada. (n) hace referencia normalmente al número de teléfono, pero hay otros códigos, por ejemplo, para generar una pausa durante la marcación del número si el módem tiene que recibir tono de marcado de una centralita. Cuando se establece la conexión, los módems cambian a modo de comunicación.

ATH – **C**olgar

El módem termina la conexión y cuelga. Para poder utilizar este comando, es necesario cambiar el módem del modo de comunicación al modo de comandos, en general con el código +++.

AT&Fn – Restaurar **la c**onfiguración de fábrica

Restaura en el módem la configuración predeterminada de fábrica o el perfil de configuración 0 ó 1.

ATQn – **O**pciones de presentación de códigos de resultado

Activa o desactiva la presentación en pantalla de los códigos de resultado enviados desde el módem. Algunas aplicaciones requieren que el módem esté configurado de modo que no se envíe ningún carácter.

ATEn – Eco activado/desactivado

Activa o desactiva el eco en el terminal conectado. Algunas aplicaciones requieren este comando, que además puede causar confusión durante la introducción de comandos.

AT&V – Visualización de la configuración actual y de los perfiles guardados

El comando muestra una lista del contenido de los perfiles y de los registros S guardados en el módem, que a su vez se utilizan para la configuración de funciones. Encontrará un ejemplo en la página 80.

AT&Wn – Guardar la configuración actual

Guarda la configuración actual del módem en el perfil 0 ó 1.

ATZn – Desconexión software y recuperación de perfil

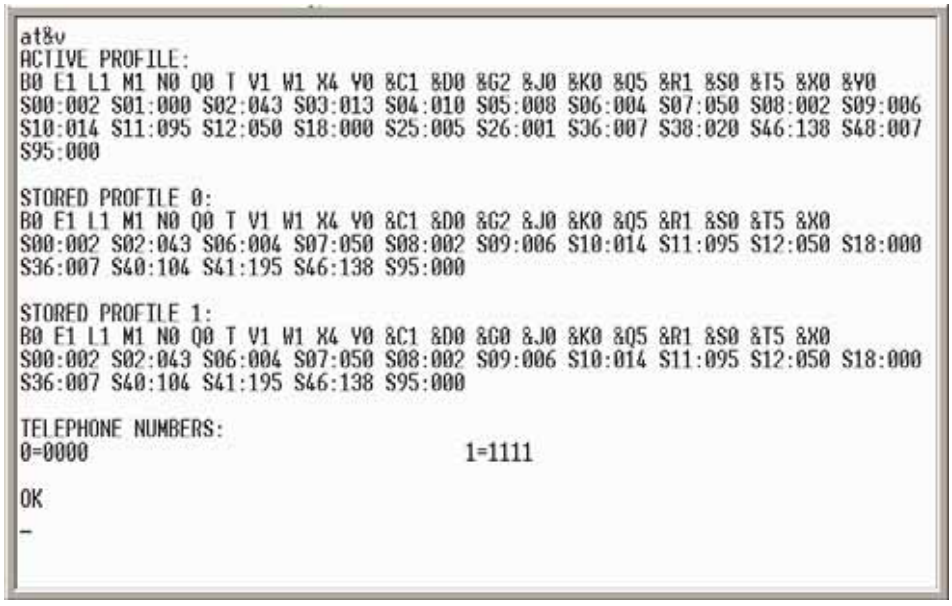
Ejecuta un reinicio de software en el módem y restablece el perfil configurado.

ATO – Modo de datos en línea

El módem cambia a modo de datos.

+++ Cambia del modo de datos en línea al modo de comandos.

La captura de pantalla con el contenido de los registros del módem y las especificaciones completas de los registros se encuentra en el manual del módem. El ejemplo siguiente describe alguna de las funciones de los registros S.



Registro	Funcionalidad
S00	El contenido del registro le indica al módem el número de señales de llamada que ha de esperar antes de responder. En este ejemplo, el módem responde después de la segunda señal de llamada, ya que el valor indicado es 002.
S01	Cuenta el número de señales de llamada entrantes.
S02	Describe qué carácter se ha de utilizar para la secuencia de escape.
S03	Describe qué carácter se ha de utilizar para el retorno de carro.
S04	Describe qué carácter se ha de utilizar para el salto de línea.
S05	Describe qué carácter se ha de utilizar para la tecla de retroceso.
S07	Describe cuántos segundos ha de esperar el módem a la portadora antes de colgar.
S10	Describe cuánto ha de esperar el módem antes de colgar cuando la portadora se ha perdido.

Mayor velocidad

xDSL

xDSL es un nombre colectivo que engloba toda una familia de tecnologías en las que los módems digitales se utilizan sobre una línea telefónica estándar o fija. La letra que sustituye a la x indica el tipo de sistema digital que viaja por la línea. Entre estas tecnologías se encuentran, por ejemplo, ADSL, SDSL, SHDSL y VDSL, cada una de las cuales es adecuada para diferentes aplicaciones. Así, VDSL puede alcanzar velocidades de transmisión de hasta 52 Mbits, pero sólo a unos 300 m, mientras que SHDSL alcanza un máximo de 2,3 Mbits a distancias de hasta 3 km, o de 192 kbit/s hasta unos 6 km.

HDSL

HDSL es la abreviatura de High speed Digital Subscriber Line (línea digital de abonado de alta velocidad). Esta tecnología ofrece comunicación dúplex a velocidades de 2,3 Mbit/s en ambas direcciones.

ADSL

ADSL es la abreviatura de Asymmetric Digital Subscriber Line (línea digital de abonado asimétrica). Esta tecnología ofrece comunicación dúplex a velocidades que alcanzan los 8 Mbit/s de bajada y los 640 kbit/s de subida y utiliza simultáneamente la línea para tráfico de voz. Para ello, el usuario debe instalar en el primer jack un filtro denominado splitter que se suele suministrar con el producto ADSL para mejorar la calidad de las transmisiones de voz por la línea. La tecnología ADSL es una opción muy popular entre los usuarios domésticos, porque la velocidad de descarga es mucho mayor que la de subida. En efecto, para los usuarios domésticos los tiempos de descarga suelen ser más importantes, pues por lo general utilizan la subida casi exclusivamente para el correo electrónico.

VDSL

VDSL es la abreviatura de Very high speed Digital Subscriber Line (línea digital de abonado de muy alta velocidad). Esta tecnología ofrece comunicación dúplex a velocidades que alcanzan los 52 Mbit/s de bajada y los 6,4 Mbit/s de subida por un par de abonado.

VDSL es la tecnología más rápida disponible actualmente para transmitir datos por la red telefónica estándar y constituye una buena alternativa a los productos ADSL cuando se necesitan velocidades de transmisión mayores para aplicaciones como:

- Vídeo en tiempo real.
- Videoconferencia.
- Combinación de vídeo y datos por la misma conexión.
- Grandes requisitos de acceso a datos.

SDSL

SDSL, abreviatura de Symmetric Digital Subscriber Loop (línea digital de abonado simétrica), y G.SHDSL son tecnologías xDSL simétricas.
Una característica que distingue a este tipo de líneas radica en que sus velocidades de subida y de bajada son similares (de ahí que se las denomine líneas simétricas). Con SDSL, el usuario puede obtener una velocidad máxima de 2,3 Mbit/s en ambas direcciones. La tecnología SDSL simétrica se puede utilizar en modo «back to back», lo que implica interconectar dos módems con cable de cobre. SDSL es una tecnología propietaria que se instala principalmente en Norteamérica. No obstante, las aplicaciones industriales ya han empezado a migrar a la norma internacional SHDSL, que se describe a continuación.

SHDSL

SHDSL es la abreviatura de Symmetric High-Bitrate Digital Subscriber Loop (línea digital de abonado simétrica de alta velocidad) y es la primera norma internacional para líneas DSL simétricas multivelocidad. Esta norma ha sido desarrollada para comunicaciones por uno o más pares trenzados. Con un solo par se alcanzan velocidades de 192 kbit/s a 2,3 Mbit/s, mientras que con dos las velocidades se encuentran entre los 384 kbit/s y los 4,6 Mbit/s. La tecnología SHDSL utiliza un algoritmo de codificación avanzado, TC-PAM, que garantiza mayores velocidades y/o distancias de transmisión que el resto de las tecnologías DSL.

Distancias de transmisión con SHDSL

	Velocidad	Distancia
Comunicación por un par		
AWG 26	192 kbit/s	6 km
Comunicación por un par		
AWG 26	2,3 Mbit/s	3 km
Comunicación por dos pares		
AWG 26	2,3 Mbit/s	5 km

Si es necesario cubrir distancias de transmisión mayores, se puede instalar un repetidor entre los dispositivos.

Encontrará información detallada en las normas:

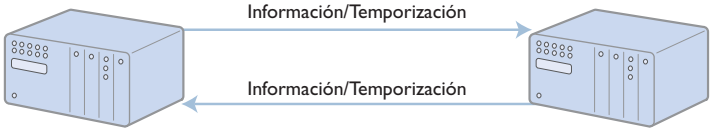
- ANSI (T1E1.4/2001-174) – Norteamérica.
- ETSI (TS 101524) – Europa.
- ITU-T (G.991.2) – Internacional.

G.703

La norma G.703 de la Unión Internacional de Telecomunicaciones (ITU) describe las propiedades físicas y eléctricas, así como varias velocidades de transmisión.
Existen tres tipos básicos de interfaz: codireccional, contradireccional y centralizada.
Esta norma especifica velocidades que van desde los 64 kbit/s hasta los 155.520 kbit/s y originalmente se elaboró para normalizar la transmisión de voz por un enlace PCM.
El medio de transmisión puede ser un par simétrico con resistencia de 120 ohmios o un cable coaxial asimétrico con resistencia de 75 ohmios.

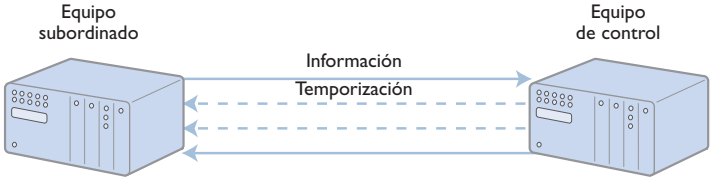
Interfaz codireccional

La transmisión utiliza un par de cable en cada sentido. La información de datos y temporización va superpuesta, se transmite en la misma dirección y es el receptor el que ha de sincronizarla.



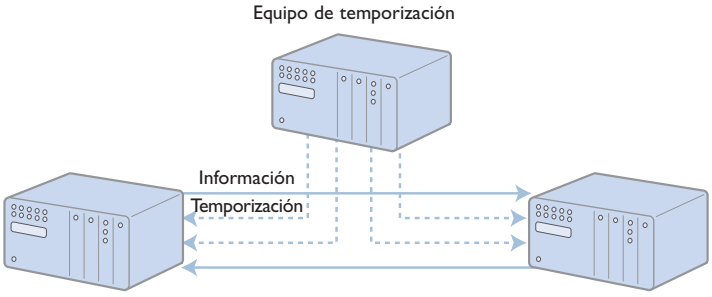
Interfaz contradireccional

Este tipo de transmisión utiliza un par de 4 hilos; la información de temporización la facilita el dispositivo de control.



Interfaz de reloj centralizado

Esta variante de la interfaz utiliza 3 ó 4 pares de cableado; la unidad central proporciona la información de temporización. En el caso de los 3 pares de cableado, la temporización es la misma para la transmisión y para la recepción. En el caso de los 4 pares de cableado, se utiliza una temporización individual para la transmisión y otra para la recepción.



GSM

GSM, GPRS, UMTS... ¿Qué significan estas expresiones y qué posibilidades de transmisión de datos ofrecen?

Las descripciones técnicas suelen estar llenas de abreviaturas y acrónimos. Para este manual hemos decidido mantener las designaciones y abreviaturas técnicas, pues, aunque suelen estar en inglés, su uso está muy generalizado.

Historia de la tecnología GSM

A comienzos de los años ochenta, en Europa se utilizaban numerosos sistemas analógicos de calidad muy diferente. Sin embargo, pronto se hizo evidente que la tecnología analógica no podría satisfacer los requisitos que una comunicación eficaz demandaría en el futuro. Para abordar el problema se creó el **G**roupe **S**pécial **M**obile (Grupo Especial de Comunicaciones Móviles), más conocido como GSM, en Viena, en el año 1982.
Este grupo recibió el encargo de desarrollar un sistema de telefonía móvil que ofreciera una elevada calidad de sonido a bajo coste.

En 1989, el **E**uropean **T**elecommunication **S**tandards **I**nstitute (Instituto Europeo de Normas de Telecomunicación, ETSI) recogió el testigo para continuar con el desarrollo de la tecnología GSM. El acrónimo GSM adquirió entonces un nuevo significado: **G**lobal **S**ystem for **M**obile communications (Sistema Global de Comunicaciones Móviles).

El sistema GSM hace posible la transmisión inalámbrica de voz, texto e imágenes entre diferentes tipos de equipos, pero únicamente si dichos equipos se encuentran dentro del área de cobertura de la estación transceptora base del operador de red. Desde la normalización, el número de usuarios de equipos GSM ha aumentado exponencialmente, sobre todo en las aplicaciones de voz. En efecto, si a comienzos del año 1994 el número de abonados era de 1,3 millones, en febrero de 2004 los usuarios de teléfonos móviles eran ya 1.024 millones en todo el mundo.

Además se está observando un gran aumento en el uso de esta tecnología en aplicaciones industriales M2M (**M**achine **to M**achine, es decir, máquina a máquina). La razón es que se puede utilizar, por ejemplo, para transmitir datos o alarmas desde unidades esclavas básicas hasta un sistema de control, o para transmitir datos desde parquímetros y entre ellos. Este campo de aplicación es prácticamente ilimitado, y los diferentes tipos de equipos GSM verán un rápido desarrollo encaminado a satisfacer las necesidades futuras.

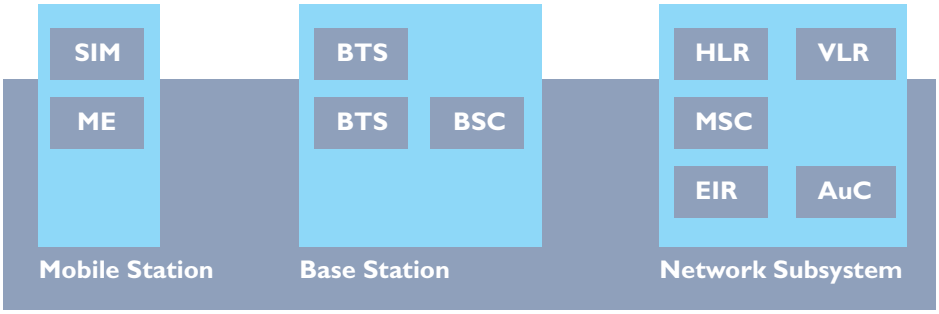
La transmisión digital utilizando tecnologías analógicas en redes de telefonía móvil presenta numerosas ventajas, entre las que cabe destacar las siguientes:

- Mejor calidad de la conexión telefónica.
- Mayores velocidades de transmisión.
- Mejor aprovechamiento del ancho de banda, lo que permite aumentar el número de abonados.
- Posibilidad de añadir nuevos servicios y funciones de datos, texto y fax.
- Posibilidad de cifrar los datos para reforzar la seguridad.
- Menor consumo de energía, con el consiguiente aumento de la autonomía de los dispositivos alimentados con baterías, tanto en conversación como en espera.

Arquitectura

La red GSM consta de tres componentes básicos:

- **M**obile **S**tation (MS, estación móvil).
- **B**ase **S**tation **S**ystem (BSS, sistema de estación base).
- **N**etwork **S**ubsystem (subsistema de red), con conexiones a redes externas como, por ejemplo, RDSI o PSTN.



Componentes de la red

ME Es el **M**obile **E**quipment (Equipo Móvil) y hace referencia a un equipo adaptado para su uso en la red GSM. Cada unidad ME tiene una identidad única (el número IMEI), que es su identificador internacional de equipo móvil y que permite al operador de red bloquear el uso de una unidad, por ejemplo, en caso de robo.

SIM Es el **S**ubscriber **I**dentity **M**odule (Módulo de Identidad del Abonado). Se trata de una tarjeta que se usa junto con la unidad ME. Suministrada por el operador de red, la tarjeta SIM contiene datos como el número de teléfono, el código PIN, la agenda telefónica, etc. La tarjeta SIM se puede instalar en cualquier unidad ME.

BTS Es la **B**ase **T**ransceiver **S**tation (Estación Transceptora Base), que es una estación base, es decir, un transmisor y un receptor que hacen posible la comunicación con algún tipo de ME.

BSC Es el **B**ase **S**tation **C**ontroller (Controlador de Estación Base). Es una subestación que se comunica con la estación base. La subestación se puede comunicar con varias estaciones base.

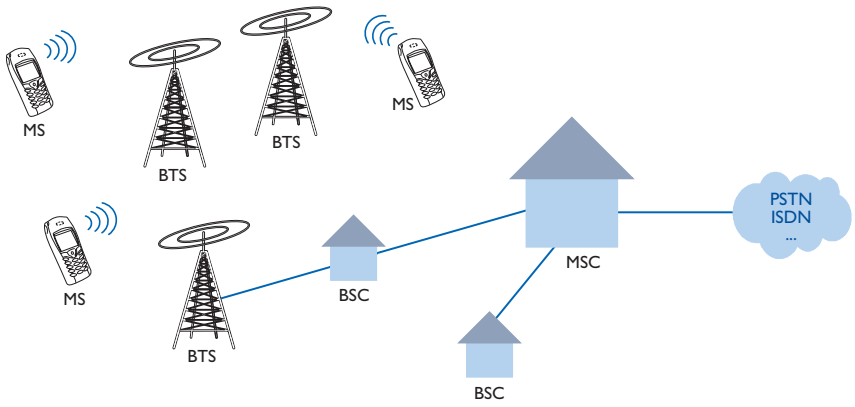
MSC Es el **M**obile **S**witching **C**entre (Centro de Conmutación de Servicios Móviles), y permite reenviar los datos a una red analógica, normalmente una red PSTN (**R**ed **T**elefónica **P**ública **C**onmutada) o una red digital RDSI (**R**ed **D**igital **de S**ervicios **I**ntegrados).

HLR Es el **H**ome **L**ocation **R**egister (Registro de Posiciones Base), una base de datos que, junto con otras, contiene información básica acerca del usuario, como el tipo de abonado.

VLR Es el **V**isitor **L**ocation **R**egister (Registro de Posiciones de Visitantes), una base de datos que almacena información acerca de un ME que se encuentra en una célula que no controla el HLR.

EIR Es el **E**quipment. **I**dentity **R**egister (Registro de Identidades de Equipos), una base de datos en la que figuran todos los usuarios de la red. La identificación se realiza mediante el número IMEI de la unidad ME.

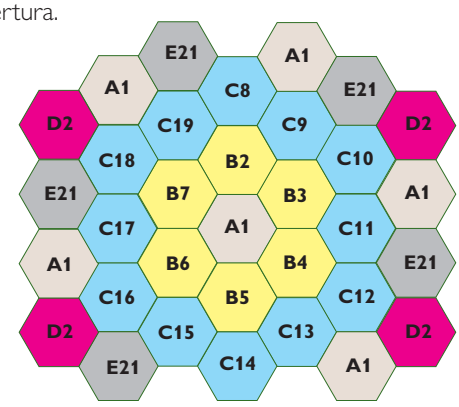
AuC Es el **Au**thentication **C**entre (Centro de Autenticación), una base de datos que contiene información sobre el operador de red y el tipo de abono del usuario.



Estructuras celulares

Las estaciones base se instalan siempre de manera que ofrezcan la máxima cobertura. El área que cubre cada estación base se denomina célula.

Toda la red GSM está organizada en células de diferentes tamaños, que van desde áreas con un radio de 200 metros hasta áreas con un radio de ~30 km. La cobertura depende del lugar en el que se encuentre la estación base y del entorno que la rodee.



Otros factores que afectan a la instalación son, entre otros, la potencia de salida y si la estación base se encuentra en un lugar problemático para las señales de radio. La principal ventaja de esta estructura celular es que las estaciones base pueden reutilizar las frecuencias. Así, tal y como se muestra en la figura, la frecuencia A1 se puede reutilizar en el tercer anillo sin riesgo de producir diafonía entre las células con la misma frecuencia.

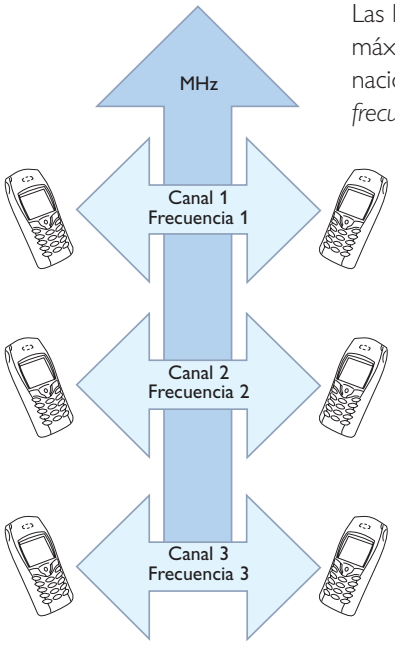
Cuando el usuario se está desplazando, se hace necesario además traspasar la llamada a las distintas células por las que pasa. Este procedimiento se conoce como «handover» (transferencia).

Transmisiones de radio entre MS y BSS

En los años ochenta, cuando se elaboró la especificación GSM, la ITU (**I**nternational **T**elecommunication **U**nion) reservó dos bandas de frecuencia de 25 MHz para las transmisiones de radio GSM:

- la banda de 880 a 915 MHz, para el «enlace ascendente» desde la MS hasta la BSS.
- la banda de 925 a 960 MHz, para el «enlace descendente» desde la BSS hasta la MS.

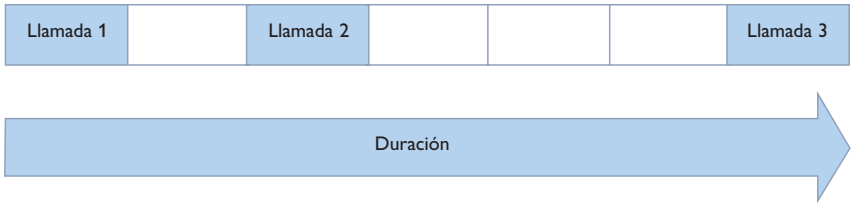
El desarrollo de las comunicaciones móviles ha supuesto la necesidad de utilizar múltiples frecuencias para satisfacer la demanda. Actualmente se utilizan cinco frecuencias normalizadas: 400, 850, 900, 1.800 y 1.900 MHz. La última se utiliza básicamente en Estados Unidos y en algunas zonas de Asia, mientras que las de 900 y 1.800 MHz están más extendidas por todo el mundo.



División en frecuencia

Las limitaciones del ancho de banda han llevado a utilizar técnicas que permitan atender al máximo número posible de usuarios simultáneamente. Para lograrlo, se utiliza una combinación de TDM, *Multiplexación por división de tiempo* y FDM, *Multiplexación por división en frecuencia.*

La división en frecuencia (FDM) reparte el ancho de banda de 25 MHz disponible en bandas de 200 KHz. En la descripción anterior sobre el reparto de las frecuencias entre las células, A1, B2, B3, etc. son ejemplos de multiplexación por división en frecuencia.



Multiplexación por división de tiempo

En la multiplexación por división de tiempo (TDM), todos los transmisores utilizan la misma frecuencia pero en intervalos temporales diferentes. Los equipos deben estar sincronizados para evitar interferencias entre los transmisores.

Resumen

Frecuencia de transmisión desde el ME a la estación base	880-915	MHz
Frecuencia de transmisión desde la estación base	925-960	MHz
Ancho de banda	35+35	MHz
Método de acceso	TDMA/FDMA	
Frecuencia por canal de radio	200	KHz
Distancia en frecuencia entre el enlace descendente y el enlace ascendente	45	MHz
Radio máximo de la célula	30	km
Radio mínimo de la célula (microcélula)	30	m
Potencia de salida máxima desde el terminal móvil	2	W @ 900 MHz

Servicios de la red GSM

La red GSM presta diversos servicios:

- Telefonía
- CSD (**C**ircuit **S**witched **D**ata, es decir, datos con conmutación de circuitos, para transmisión de datos).
- SMS (**S**hort **M**essage **S**ervice, servicio de mensajes cortos).
- MMS (**M**ultimedia **M**essage **S**ervice, servicio de mensajes multimedia).
- FAX.
- GPRS (**G**eneral **P**acket **R**adio **S**ervice, servicio general de radiocomunicaciones por paquetes).

Telefonía

Es el servicio GSM más común y el que ha propiciado la rápida expansión de esta tecnología en todo el mundo. Los algoritmos que codifican y descodifican el tráfico han estado en constante desarrollo, lo que ha conducido a una reducción permanente al mínimo del ancho de banda para telefonía, sin alterar la calidad de la transmisión.

Servicio de transmisión de datos con conmutación de circuitos

En la transmisión de datos se pueden alcanzar velocidades de 2.400 bit/s a 14,4 kbit/s. La tabla muestra las velocidades y los protocolos disponibles.

La transmisión de datos se puede configurar para transferir datos de modo transparente o no transparente. El segundo tipo utiliza RLP (**R**adio **L**ink **P**rotocol, protocolo de enlace de radio), un protocolo GSM con corrección de errores. Este protocolo aumenta la fiabilidad de las transmisiones, si bien a costa de cierto retraso. Para utilizar esta función es necesario contar con el servicio y que los dispositivos conectados sean compatibles con él.

Velocidad	Protocolo
2.400 bit/s	V.22 bis
4.800 bit/s	V.32
9.600 bit/s	V.32
14.400 bit/s	V.32 bis
2.400 bit/s	V.110
4.800 bit/s	V.110
9.600 bit/s	V.110
14.400 bit/s	V.110

SMS

Es el servicio más utilizado después de la telefonía. El servicio SMS utiliza el canal de la señal para transmitir mensajes de texto. Este servicio ha adquirido popularidad tanto para uso personal como profesional debido a su sencillez. De forma resumida, sus características básicas son las siguientes:

- El mensaje puede tener hasta 160 caracteres.
- La transmisión no está garantizada, ya que el receptor puede tener el teléfono apagado o encontrarse fuera de cobertura. Además, el servicio ofrece distintas posibilidades de configuración del mensaje:
- Permanencia del mensaje en la red cuando no llega inmediatamente al receptor (hasta una semana).
- Confirmación de la recepción, por ejemplo, el emisor recibe confirmación de que el mensaje ha llegado a su receptor.
- Acuse de recibo de envío del mensaje.
- Posibilidad de enviar y recibir SMS durante una llamada.
- Posibilidad de enviar mensajes SMS a destinatarios individuales o a grupos de destinatarios.

MMS

MMS es la abreviatura inglesa de **M**ultimedia **M**essaging **S**ervice (Servicio de Mensajes Multimedia) y funciona del mismo modo que los mensajes SMS, pero con opciones para:

- Enviar imágenes y animaciones.
- Enviar música.
- Grabar y enviar mensajes de voz propios.
- Escribir mensajes de texto largos.
- Enviar mensajes que contengan miles de caracteres, según el modelo de teléfono móvil.

Fax

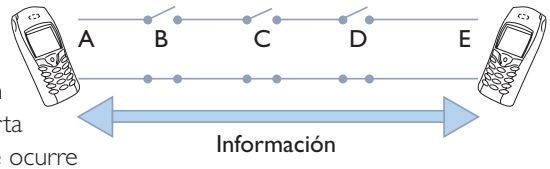
Disponible para faxes de clase 1 y de clase 2.

GPRS

GPRS es una evolución de la red GSM que posibilita la transmisión de datos con conmutación de paquetes. Se trata de una tecnología diferente de la de transmisión de datos con conmutación de circuitos, utilizada por GSM. Con GPRS, cada canal que no está ocupado con tráfico de voz se puede utilizar para la transmisión de datos con conmutación de paquetes. Además, permite combinar paquetes de distintos usuarios en el mismo canal, lo que aumenta la eficiencia de uso de los recursos de red disponibles.

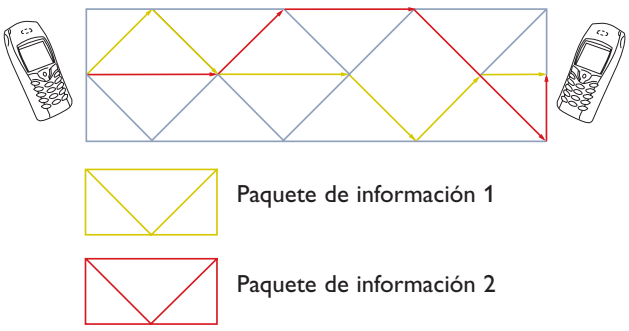
GPRS puede ofrecer velocidades de transmisión aún mayores, porque utiliza varios intervalos de tiempo para la transmisión. En teoría se pueden conseguir velocidades de hasta 115,2 kbit/s, aunque lo normal es que oscilen entre 20 y 50 kbit/s (en comparación con ésta, la transmisión de datos con conmutación de circuitos a alta velocidad HSCSD, *High Speed Circuit Switched Data* que ofrecen algunos operadores para la transmisión con conmutación de circuitos por la red GSM permite velocidades de 9,6 a 43,2 kbit/s). Sin embargo, la velocidad de transmisión depende de factores como el operador, el terminal, el número de usuarios que se encuentran en la misma célula, la distancia a la estación base (retransmisiones), si el dispositivo está en movimiento (el paso de una estación base a otra reduce la velocidad), etc.

La velocidad de transmisión también depende del número de intervalos de tiempo en uso, así como del sistema de codificación que esté utilizando el enlace de comunicación. GPRS tiene 4 **C**oding **S**chemes (CS) (procedimientos de codificación). Así, CS1 es el más seguro y el más fiable, pero también es el que ofrece la velocidad de transmisión más baja (9,05 kbit/s), mientras que CS4 no tiene una corrección de errores y de retransmisiones tan estricta, por lo que alcanza velocidades de 21,4 kbit/s. Las velocidades dependen del número de intervalos de tiempo y del procedimiento de codificación, lo que quiere decir que 4 intervalos de tiempo en CS4 producen 4 x 21,4 = 85,6 kbit/s. Además, conviene saber que, aunque la norma GSM especifica 4 procedimientos de codificación, sólo los dos primeros, CS1 y CS2, (13,4 kbit/s por intervalo de tiempo) están implantados actualmente en las redes GSM activas.



La diferencia entre las redes con conmutación de circuitos y con conmutación de paquetes puede describirse, de forma resumida, como sigue:

En la **red con conmutación de circuitos** se establece una conexión física entre las dos partes. Esta conexión está constantemente abierta y no se cierra hasta que una de las partes así lo decide, al igual que ocurre con las llamadas telefónicas. Este método tiene ventajas y desventajas. Las unidades en comunicación tienen una conexión continuada entre sí, detectan la capacidad disponible y saben que no será utilizada por ningún otro usuario. Por otro lado, se produce un gasto de recursos innecesario cuando las partes no están intercambiando información, ya que la línea está ocupada y ninguna otra persona puede utilizarla. Por consiguiente, las partes deben finalizar la conexión cuando no la van a utilizar más.



En la **red con conmutación de paquetes** el tráfico se divide en pequeños paquetes que se envían a través de la red, de manera que otros usuarios pueden utilizarla al mismo tiempo. Así, del mismo modo que el funcionamiento de la red con conmutación de circuitos se puede asimilar a una llamada telefónica, el de la red con conmutación de paquetes es parecido al de una empresa de transportes o una oficina de correos: varias personas pueden enviar muchos paquetes al mismo tiempo. La oficina de correos o el transportista se aseguran de que todos los paquetes lleguen a su destinatario, y los paquetes comparten los camiones e instalaciones durante el recorrido.

En febrero de 2004 había 172 operadores en todo el mundo que ofrecían la opción de GPRS. Se espera que el número de teléfonos móviles con GPRS pase de los 10 millones de 2001 a 280 millones en 2005.

Seguridad de las redes

GSM

Los mecanismos de seguridad más importantes de la red GSM son los siguientes:

- Potente autenticación de los usuarios (la red autentica la tarjeta SIM, la tarjeta SIM autentica al usuario con el código PIN).
- Protección contra la captación de datos (escucha) en la interfaz de radio.
- Protección contra la captación de señales en la interfaz de radio.
- Verificación de la identidad de la unidad, lo que permite bloquearla en caso de robo.

Cifrado de datos en la conexión de radio, por ejemplo, entre la unidad y la estación base. La clave secreta de cada usuario se guarda en la tarjeta SIM, la principal central de autentificación del operador.

GPRS

Básicamente utiliza los mismos mecanismos de seguridad que la tecnología GSM. La autenticación se realiza de la misma manera, pues se puede utilizar la misma tecnología de autenticación y la tarjeta SIM. Sin embargo, las claves criptográficas generadas son siempre diferentes para GSM y para GPRS, ya que GPRS utiliza algoritmos de cifrado especiales, con claves de 64 bits.

Diferencias entre GSM y GPRS

CSD
Datos **con** **C**onmutación de **C**ircuitos
TDM
Multiplexación **por** **D**ivisión **de** **T**iempo

1	2	3	4	5	6	7	8

Se utiliza un intervalo de tiempo que garantiza una velocidad máxima de 14,4 kbit/s.

El coste de explotación se basa en la duración de la conexión, sea cual sea la cantidad de datos enviados.

GPRS
Servicio **G**eneral de **R**adiocomunicaciones por **P**aquete
TDM
Multiplexación por **D**ivisión de **T**iempo

1	2	3	4	5	6	7	8

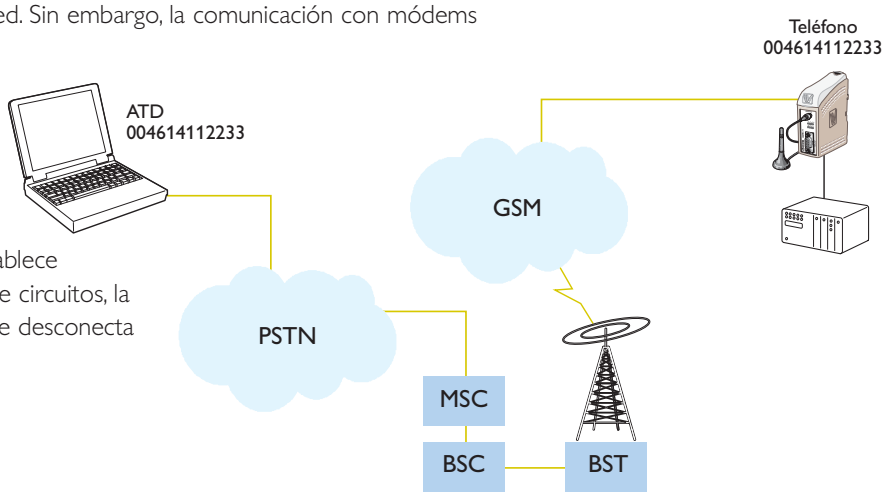
Con cuatro intervalos de tiempo y el procedimiento de codificación 4, la velocidad máxima es de 85,6 kbit/s.

El coste de explotación está basado en la cantidad de datos enviados (número de paquetes), sea cual sea el tiempo de conexión.

Aplicaciones con GSM y GPRS

La posibilidad de utilizar GSM y GPRS en la transmisión de datos es una alternativa a la comunicación por radio. Las aplicaciones inalámbricas se utilizan principalmente cuando no hay líneas dedicadas o conexiones de red. Sin embargo, la comunicación con módems GSM o GPRS requiere algunas condiciones básicas.

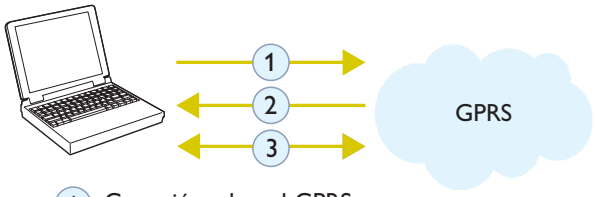
El módem GSM se conecta a la red GSM estableciendo una conexión a través del MSC y el BSC hacia el exterior por una línea PSTN del ordenador. Dado que la conexión GSM se establece a través de una red con conmutación de circuitos, la conexión no se interrumpe hasta que se desconecta la línea.



La comunicación mediante GPRS utiliza otro procedimiento. En efecto, la tecnología GPRS está basada en IP y la unidad conectada debe facilitar una dirección IP para que pueda establecerse una conexión.

El procedimiento completo incluye los pasos siguientes:

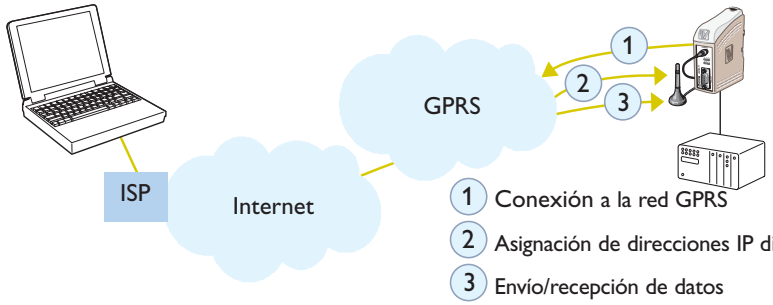
- Conexión a la red GPRS.
- Asignación de una dirección dinámica.
- Intercambio de datos.



1. Conexión a la red GPRS
2. Asignación de direcciones IP dinámicas
3. Envío/recepción de datos

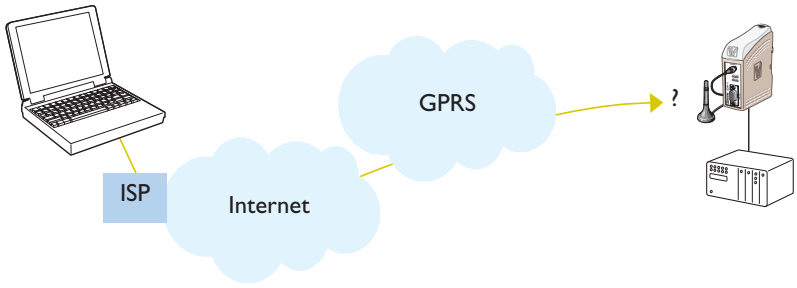
A día de hoy no todos los operadores pueden ofrecer opciones de abono con asignación de direcciones estáticas. En la asignación dinámica, el usuario no sabe qué dirección se asigna al otro equipo en cada caso.

Esto no es un problema si el módem GPRS está conectado al maestro, pues éste toma la iniciativa en la conexión y el módem tiene su dirección IP asignada, lo que significa que se puede establecer una conexión con un equipo que tiene una dirección IP fija, por ejemplo un ordenador.

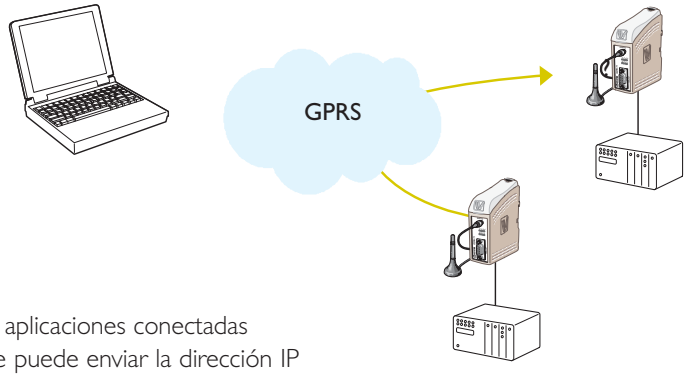


1. Conexión a la red GPRS
2. Asignación de direcciones IP dinámicas
3. Envío/recepción de datos

El problema se produce cuando una unidad, por ejemplo un ordenador, quiere comunicarse con un periférico y el ordenador establece la conexión. Como las direcciones IP se asignan dinámicamente, ningún elemento sabe a cuál debe conectarse el ordenador.

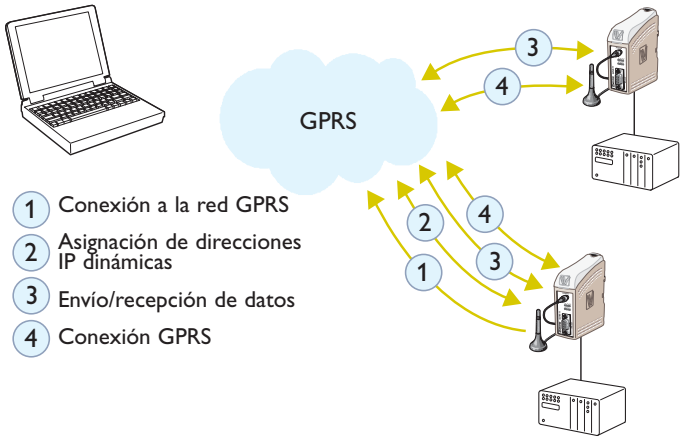


El mismo tipo de problema se presenta en las aplicaciones en las que dos dispositivos han de comunicarse y ninguno de ellos es el maestro. El módem no puede iniciar la comunicación IP, ya que no sabe qué dirección se asignará.



Existen soluciones para este problema, pero las aplicaciones conectadas deben ser compatibles con ellas. Por ejemplo, se puede enviar la dirección IP asignada a la contraparte en un mensaje corto.

No obstante, hay que ser consciente de que, si alguno de los dispositivos conectados sufre un fallo de alimentación, será necesario repetir el procedimiento porque la dirección IP se habrá perdido.



1. Conexión a la red GPRS
2. Asignación de direcciones IP dinámicas
3. Envío/recepción de datos
4. Conexión GPRS

Clases de GPRS

Actualmente hay equipos GPRS de tres categorías, definidas como Clase A, B y C.

Clase A	Admite operaciones GSM y GPRS simultáneas
Clase B	Admite operaciones GSM y GPRS, pero no simultáneas.
Clase C	La conexión sólo es compatible con datos GPRS o GSM. Para cambiar entre GPRS y GSM, hay que volver a establecer la conexión.

Clases multislot con 1 a 5 slots de tiempo

	Número máximo de slots		
Clase Multislot GPRS	RX "downlink"	TX "uplink"	Máx.
Clase 1	1	1	2
Clase 2	2	1	3
Clase 4	3	1	4
Clase 6	3	2	4
Clase 8	4	1	5
Clase 10	4	2	5
Clase 11	4	3	5
Clase 12	4	4	5

RX: Número máximo de slots de tiempo recibidos que admite la MS por trama TDMA en GSM.

TX: Número máximo de slots de tiempo que la MS puede enviar por trama TDMA en GSM.

Máx: Número total de slots de tiempo en los enlaces de "uplink" y "downlink" que puede utilizar de manera simultánea la MS en la trama TDMA.

UMTS (3G)

3G es el nombre con que se suele hacer referencia a la norma conocida como UMTS (**U**niversal **M**obile **T**elecommunications **S**ystem, sistema universal de comunicaciones móviles), que describe la tecnología en la que se basa el sistema de telefonía de tercera generación. En algunos países, 3G puede implicar otras normas. La expresión 3G tiene su origen en el hecho de que es la tercera generación de telefonía móvil. La primera generación fue analógica, luego vino el GSM, que es el sistema más común actualmente y ahora se acaba de lanzar la 3G.

La principal diferencia entre 3G y GSM es la capacidad de transmisión, es decir, la rapidez con la que el teléfono puede enviar y recibir datos. Cuanto mayor sea la velocidad de transmisión, más servicios podrá ofrecer la red móvil. En la tecnología 3G, la velocidad es unas 40 veces superior, lo que permite acceder a servicios avanzados como el envío y la recepción de imágenes, la transmisión de imágenes animadas y el uso de servicios basados en la ubicación del usuario. Por eso esta tecnología recibe también el nombre de banda ancha móvil.

RDSI

¿Qué es RDSI?

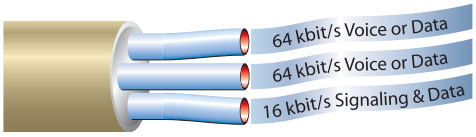
Del inglés ISDN (**I**ntegrated **S**ervices **D**igital **N**etwork), la red digital de servicios integrados es el equivalente digital de la red telefónica estándar PSTN (**P**ublic **S**witched **T**elephone **N**etwork, red pública telefónica conmutada). La tecnología RDSI está normalizada según las recomendaciones de la **U**nión **I**nternacional de **T**elecomunicaciones (ITU).

Señalización

En lugar de que la compañía telefónica active la señal de llamada del teléfono (señal en banda), se envía un paquete digital por un canal distinto (señal fuera de banda). La señal fuera de banda no perturba la llamada en curso, tiene un tiempo de conexión corto y contiene información sobre el emisor de la llamada, el tipo de llamada (voz o datos) y el número llamante. A continuación, el equipo RDSI disponible determina cómo se debe gestionar la llamada.

Conexiones

La conexión RDSI se compone de varios canales B que transportan básicamente datos, y un canal D principalmente para señales de control. La velocidad de transmisión de datos en un canal B es de 64 kbit/s, aunque para aumentar la velocidad se pueden interconectar varios canales. Los clientes suelen tener acceso a RDSI con dos tipos de abonos diferentes. El acceso básico, que comprende dos canales B básicos y un canal D de 16 kbit/s (2B+D), ofrece una velocidad máxima de dos veces 64 kbit/s (es decir, 128 kbit/s), adecuada para usuarios que requieren mayores velocidades de transmisión de datos o que desean combinar la comunicación telefónica, las llamadas de fax y la transmisión de datos, así como para pequeñas redes locales. Es posible conectar hasta 8 dispositivos RDSI a la misma línea, algo que resulta de gran utilidad si la conexión RDSI incluye dispositivos de distintos tipos.



Los dispositivos reciben números individuales de la misma manera que si tuvieran su propia conexión a la red. El acceso primario comprende 30 canales B y un canal D de 64 kbit/s (30B+D). La capacidad máxima cuando están conectados los 30 canales es de 2 Mbit/s. El acceso primario RDSI es adecuado para conectar ordenadores cuando se necesita una velocidad de transmisión de datos elevada (por ejemplo, para videoconferencia), así como en grandes redes locales, switches digitales y puentes entre grandes redes regionales.

Las mayores ventajas de la conexión RDSI son la velocidad de transmisión (64–128 kbit/s), los tiempos de conexión (inferiores a 2 segundos), la estabilidad de las conexiones, la menor sensibilidad a las interferencias y la flexibilidad derivada de poder conectar múltiples dispositivos a la misma línea (por ejemplo, teléfono, fax u ordenador).

Interfaz/componentes de las líneas RDSI

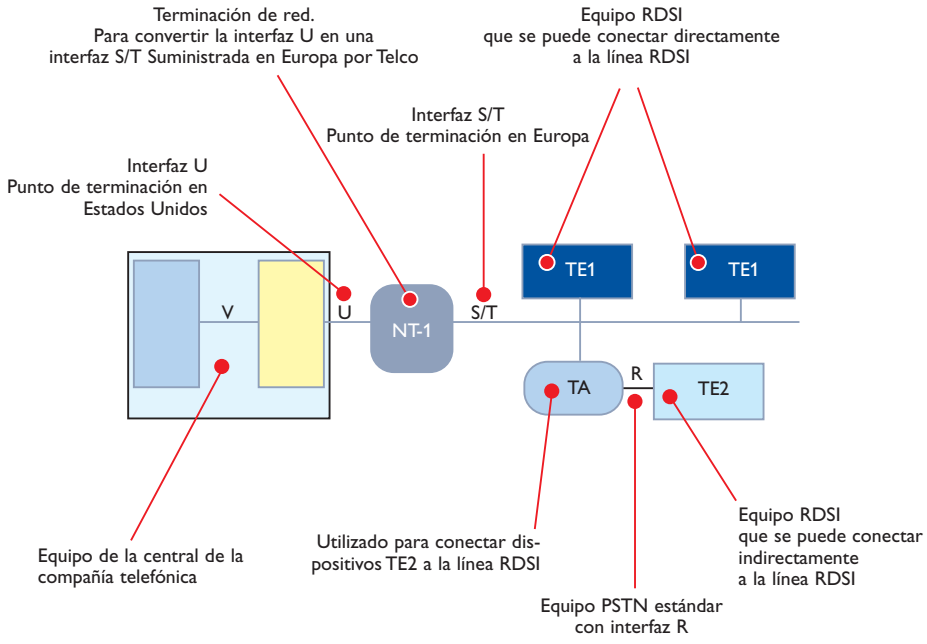
Los componentes de la línea RDSI incluyen terminales, adaptadores de terminal (TA), dispositivos de terminación de red (NT), equipos de terminación de línea (LT) y equipos de terminación de central (CLA). Los terminales pueden ser de dos tipos: terminales RDSI especializados con interfaz RDSI, conocidos como equipos terminales de tipo 1 (TE1), y terminales con interfaz distinta a la RDSI, esto es, unidades con interfaz V.24, conocidas como equipos terminales de tipo 2 (TE2). El equipo TE1 se conecta a la red RDSI por un «par trenzado» digital de 4 hilos, mientras que el equipo TE2 se conecta a través de un adaptador de terminal. Este último puede ser un dispositivo autónomo o una tarjeta de interfaz instalada en el dispositivo TE2. Cuando el equipo TE2 y el adaptador de terminal (TA) son independientes, se suele utilizar una interfaz normalizada como RS-232/V.24 o V11/RS-485.

La siguiente interfaz en sentido ascendente hacia la línea es la de terminal de red, que enlaza la interfaz de 4 hilos del cliente con los cables de cobre convencionales de 2 hilos del operador de servicios de telecomunicaciones.

Los terminales de red también pueden ser de dos tipos: NT1 y NT2. Los de tipo NT2 son más complejos y forman las capas 2 y 3, con funciones de protocolo y concentración. Este tipo de terminales es habitual, por ejemplo, en las centralitas de las oficinas. En la mayoría de los países, los terminales de red pertenecen al operador de servicios de telecomunicaciones.

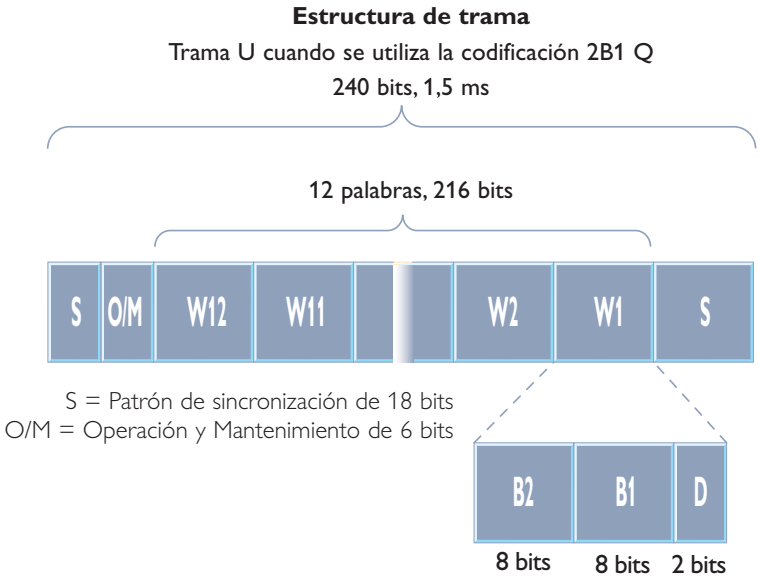
El modelo de referencia para RDSI incluye varios puntos de referencia establecidos que conforman la interfaz entre los dispositivos/terminales del modelo de referencia de conformidad con lo siguiente:

- R --- Punto de referencia que conforma la interfaz entre los dispositivos no RDSI y los adaptadores de terminal (TA) de norma RS-232/V.24.
- S --- Punto de referencia que genera la interfaz entre el TE/TA y el NT1.
- T --- Punto de referencia que forma la interfaz entre los dispositivos NT1 y NT2.
- U --- Punto de referencia que forma la interfaz entre el NT1 y el terminal de línea LT.



Capa física

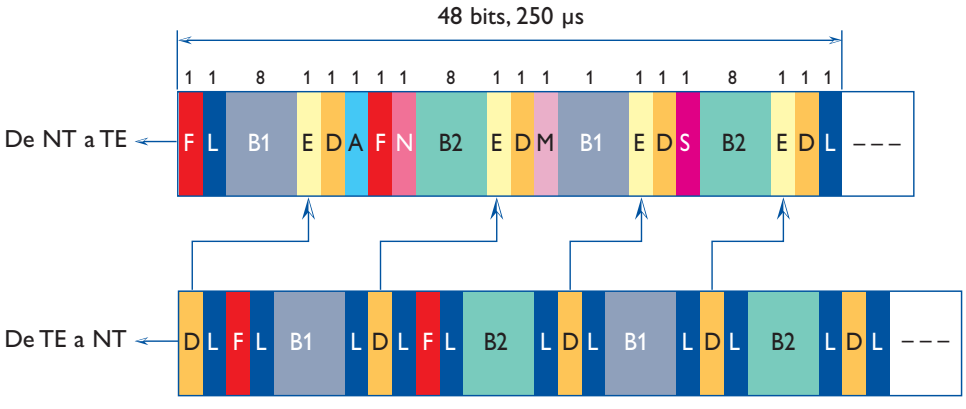
La señalización entre el terminal de línea de la central de telecomunicaciones (LT) y el terminal de red del usuario (NT) se realiza mediante la interfaz U, mientras que la señalización en las instalaciones del usuario, entre el NT y el adaptador de terminal TA, se realiza mediante la interfaz S. La interfaz U utiliza tramas de 240 bits, que se transfieren a una velocidad de 160 kbit/s. Las tramas de la interfaz U se estructuran tal y como se muestra en la figura que aparece a continuación.



Formato de trama en la interfaz S

Las tramas de la interfaz S utilizan 48 bits, de los cuales 36 se utilizan para la transmisión de datos. La velocidad de transmisión de la interfaz S es de 192 kbit/s. La estructura interna de las tramas difiere ligeramente dependiendo de la dirección de envío. La figura muestra cómo se utilizan los diferentes bits.

A = Bit de activación
B1 = Canal B1 (2 x 8 bits/trama)
B2 = Canal B2 (2 x 8 bits/trama)
D = Canal D (4 x 1 bit/trama)
E = Eco del bit D anterior
F = Bit de alineación de trama
L = Equilibrado de CC
S = Canal S
N = F invertido de NT a TE
M = Bit de alineación de trama múltiple



Capa 2 – Capa de enlaces de datos

La capa de enlace de datos para RDSI está definida en las normas Q.920 a Q.923 de la ITU. Más concretamente, el documento Q.921 define la señalización del canal D. Esta capa utiliza el protocolo Link Access Procedure – D channel (LAP-D, procedimiento de acceso al enlace en el canal D), que es casi idéntico al protocolo LAP-B de X.25, pues ambos se basan en HDLC. En LAP-D, la estructura de las tramas es la siguiente:

Bandera	Dirección	Control	Información	CRC	Bandera

Bandera (1 byte)
La bandera inicial es siempre 7E16 (0111 11102).

Dirección (2 bytes)

8	7	6	5	4	3	2	1
SAPI (6 bits)						C/R	EA0
TEI (7 bits)							EA1

SAPI (**S**ervice **A**ccess **P**oint **I**dentifier = Identificador de punto de acceso al servicio), 6-bits.
C/R (**C**ommand/**R**esponse = Comando/Respuesta), bit que indica si la trama es un comando o una respuesta.
EA0 (**A**ddress **E**xtension = Ampliación de dirección), bit configurado para indicar el último byte en una dirección.
TEI (**T**erminal **E**ndpoint **I**dentifier = Identificador de punto extremo terminal), identificador de dispositivo de 7 bits (consulte la página 102).
EA1 (Address Extension = Ampliación de dirección), bit con la misma funcionalidad que EA0.

Control (2 bytes)
El campo de control se utiliza para mostrar el tipo de trama y el comando. Hay tres tipos diferentes de tramas: información, supervisión/control y tramas no numeradas; las dos primeras también incluyen los números de secuencia (N[r] y N[s]).

Información
Este campo contiene información para el nivel de red superior y datos de usuario.

CRC (2 bytes)
Suma de comprobación (checksum) por redundancia cíclica de 16 bits para detectar bits incorrectos en la transmisión.

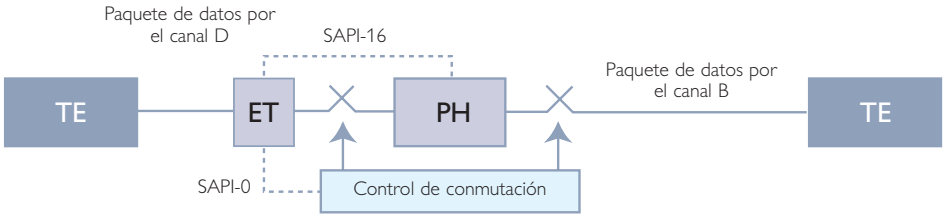
Bandera (1 byte)
La bandera final es siempre 7E16 (0111 11102).

SAPI

El identificador de punto de acceso al servicio es un campo de 6 bits que permite especificar hasta 64 funciones de servicio diferentes que el nivel 2 facilita al nivel 3.

Valor SAPI	Capa 3 relacionada o entidad de gestión
0	Procedimientos de control de las llamadas
1–11	Reservado para futura normalización
12	Información de teleacción
13–15	Reservado para futura normalización
16	Transmisión de paquetes según los procedimientos de X.25 (nivel 3)
17–31	Reservado para futura normalización
63	Procedimientos de gestión de la capa 2
Todos los demás	No disponible para procedimientos Q.921

La figura ofrece una panorámica del uso del campo SAPI, con SAPI = 0 para control de conmutación y SAPI = 16 para encaminamiento de paquetes cuando se utiliza X.31 (X.25 por el canal D).



TEI

El identificador de punto extremo terminal (TEI) es una identidad única que se asigna a cada TA/TE del bus S/T de RDSI. La asignación puede ser dinámica, cuando el dispositivo se activa, o estática, durante la instalación.

Valor TEI	Tipo de usuario
0–63	Equipo de usuario con asignación de TEI no automática
64–126	Equipo de usuario con asignación de TEI automática
127	Difusión a todos los dispositivos

Capa 3 – Capa de red

La capa de red para RDSI está definida en las normas ITU Q.930 a Q.939. Esta capa es la encargada de establecer, mantener y terminar las conexiones lógicas entre dos dispositivos. La estructura del campo de información de la capa 3 es de longitud variable, y los diferentes campos están especificados en Q.931:

Campo de información							
8	7	6	5	4	3	2	1
Discriminador de protocolo							
0	0	0	0	Longitud de CRV			
Valor de referencia de llamada (1 o 2 bytes)							
0	Tipo de mensaje						
Elementos de información obligatorios y opcionales (variable)							

La cabecera del mensaje del campo de información tiene este aspecto:

Discriminador de protocolo (1 byte)

El campo identifica el tipo de protocolo utilizado para gestionar mensajes de la capa 3. Con Q.931, este campo es 0816.

Longitud (1 byte)

Longitud del campo posterior.

Valor de referencia de llamada (CRV) (1 ó 2 bytes)

Este campo se utiliza para identificar la llamada/conexión a la que pertenece el mensaje de señalización. Se sigue utilizando el mismo valor mientras la llamada en curso sigue activa.

Tipo de mensaje (1 byte)

Este campo indica el tipo de mensaje enviado. Los mensajes pueden pertenecer a los cuatro grupos siguientes: conexión, información, desconexión y otros mensajes. SETUP y CONNECT pertenecen al primer grupo. Elementos de información (longitud variable). El contenido de este campo consiste en varios elementos de información. El tipo de elemento de información enviado depende del campo anterior (tipo de mensaje). Así, pueden ser elementos de información de número B, servicios adicionales, requisitos de la transmisión por la red, etc.

CAPI

COMMON-ISDN-API (CAPI) es una interfaz normalizada para diseñar aplicaciones de software que utilicen RDSI. La norma CAPI permite desarrollar aplicaciones capaces de comunicarse por RDSI sin tener que tener en cuenta las implementaciones específicas del fabricante de la línea RDSI.

Hoy día casi no se trabaja con esta norma, y la mayoría de los operadores de telecomunicaciones ofrecen RDSI basada en Q931/**ETSI 300 102**, que es la versión 2.0 de CAPI desarrollada para soportar el protocolo basado en Q 931. Con los años, CAPI se ha convertido en la base de muchas pilas de protocolos diferentes para redes, telefonía y transferencia de archivos.

Actualmente, está integrada en la norma europea ETS 300 838 «**I**ntegrated **S**ervice **D**igital **N**etwork (ISDN); Harmonized Programmable Communication Interface (HPCI) for ISDN».

Radio

Comunicación por radio

La transmisión inalámbrica de datos a través de un módem de radio proporciona un medio para establecer comunicaciones con:

- unidades remotas.
- estaciones de medición.
- edificios externos e instalaciones sin personal.
- centros temporales o móviles.

El propósito puede ser recopilar resultados de pruebas, controlar o regular equipos o grabar alarmas de diverso tipo.

Las tecnologías de radiocomunicación y los métodos de planificación, dimensionamiento y eliminación del ruido y las interferencias difieren mucho de las comunicaciones locales en una red de datos.

Funcionamiento de la comunicación por radio

El equipo de comunicación utiliza un módem de radio que convierte la señal de datos en ondas de radio para un canal específico con un ancho de banda concreto. La señal de datos puede requerir alguna forma de procesamiento o filtrado de la señal antes de su transmisión por el canal de radio. Además, la señal se modula (en un módem) a una frecuencia de portadora correcta y se puede transmitir por un enlace de radio hasta el receptor. Tanto si la fuente es analógica como si es digital, la transmisión suele ser siempre analógica. El equipo receptor descodifica y reconstruye la señal original.

El rango de frecuencias disponible para las comunicaciones por radio está limitado y regulado en un convenio internacional (ITU).

Las ondas de radio se propagan por la atmósfera en la capa entre la ionosfera y la superficie de la tierra. Las condiciones de comunicación pueden variar enormemente según la banda de frecuencias, y van desde las longitudes de onda más largas (hasta 1.000 metros) en la banda ELF a las más cortas (10 mm) en la banda EHF. Los módems de radio trabajan en la banda UHF, a unos 440 MHz. Esta banda va de 300 a 3.000 MHz e incluye también emisiones de radar, radio, TV, telefonía móvil NMT, radio móvil, comunicaciones por satélite, transmisiones de radioaficionados y teléfonos GSM e inalámbricos.

Banda de frecuencias

ELF	300–3000 Hz
VLF	3–30 kHz
LF	30–300 kHz
MF	300–3000 kHz
HF	3–30 MHz
VHF	30–300 MHz
UHF	300–3000 MHz
SHF	3–30 GHz
EHF	30–300 GHz

Atenuación y ruido

Al propagarse, la onda de radio se ve afectada por las capas de tierra y aire que atraviesa. En las bandas de frecuencia en las que trabajan los módems de radio, con longitudes de onda que rondan el metro, hay colinas y edificios que pueden provocar una sombra en la transmisión de las ondas (consulte la sección dedicada a la telefonía móvil), que viene a añadirse a las interferencias intermitentes derivadas de otros equipos. Este tipo de interferencia provocada por objetos se conoce como sombra o desvanecimiento de la señal, y se traduce en una amortiguación o distorsión de ésta.

Con todo, aunque la señal que llega al receptor suele ser muy débil en comparación con la señal transmitida, en sí mismo este fenómeno no implica deterioro alguno de la comunicación. En cambio, las interferencias fuera de control el ruido que se añade a la señal sí pueden ser una fuente de problemas. Además, este tipo de ruido no sólo se produce en el equipo receptor, sino que también puede presentarse en forma de ruido térmico (movimiento térmico de las partículas), ruido atmosférico (fenómenos eléctricos como rayos), ruido cósmico (radiación de radiofrecuencia procedente del Sol y otros tipos de lo que se conoce como ruido galáctico) y ruido local (equipos eléctricos situados cerca del receptor).

Antenas

Terminología

Para hablar de las comunicaciones por radio y las antenas, antes es preciso comprender algunos conceptos y expresiones fundamentales. La primera fórmula básica es la que relaciona la frecuencia (f) con la longitud de onda (l) mediante la ecuación: l [m] = 300 / f [MHz].

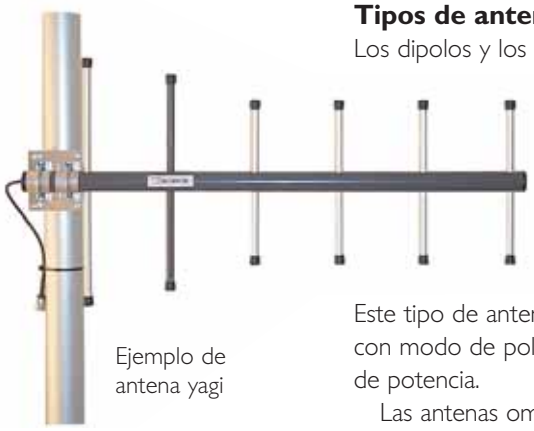
El diagrama de radiación (o directividad) de una antena es su característica de radiación tridimensional en 2 planos: el campo eléctrico (E) y el campo magnético (H). Por su parte, la ganancia de la antena es su capacidad para concentrar la radiación en una dirección específica en el espacio, a expensas de otras direcciones. La ganancia se expresa en dB frente a una referencia. Por ejemplo, dBi hace referencia a la ganancia respecto de una antena isotrópica, y dBd se refiere a la ganancia en comparación con una antena dipolo. Otro concepto clave es el de polarización, que se define como el plano del campo eléctrico (E) de la antena y que puede ser vertical, horizontal, oblicuo o circular. Por lo general, la orientación física de la antena coincide con su polarización. La polarización ortogonal tiene una pérdida por polarización cruzada de 21 dB. En la práctica, todas las antenas de un sistema deben utilizar la misma polarización.

La impedancia de una antena es su resistencia CA y su reactancia dentro de la gama de funcionamiento. El valor normalizado de impedancia nominal es de 50 ohmios. El ancho de banda es la gama de frecuencias en la que características de la antena como la impedancia, la ganancia y el diagrama de radiación se mantienen dentro de las especificaciones. Por último, el término atenuación, de uso común, está relacionado básicamente con las líneas de alimentación y la propagación radioeléctrica, y también se expresa en dB.

La antena y sus componentes

Una antena es un dispositivo electromecánico cuya finalidad es radiar con la mayor eficacia posible y de una manera específica la potencia de la línea de alimentación.

El splitter de potencia combina múltiples cargas o fuentes y reparte equitativamente la potencia entre ellos sin modificar la impedancia característica del sistema. Los splitters se utilizan en sistemas de antenas, para combinar varias antenas, así como en arneses de distribución RF. La línea de alimentación es un cable que interconecta el equipo de radio y la antena. Se trata de un componente delicado, por lo que hay que seleccionarla cuidadosamente en función de la longitud y la frecuencia de trabajo necesarias. Entre el equipo de radio y la línea de alimentación se pueden instalar pararrayos para proteger el equipo de radio de los rayos. Normalmente, el pararrayos es una varilla de cuarto de onda cortocircuitada en CC. Al interconectar los componentes del circuito de antena, es imprescindible mantener la adaptación de impedancia para garantizar un flujo ideal de potencia sin pérdidas adicionales provocadas por las reflexiones. La adaptación de impedancia se suele medir como la relación de onda estacionaria (VSWR, **V**oltage **S**tanding **W**ave **R**atio), y se considera que una VSWR de 1:1 es ideal, aunque un valor de 1:1,5 resulta más realista en la práctica.



Ejemplo de antena yagi

Ejemplo de antena dipolo

Tipos de antenas

Los dipolos y los sistemas de antenas dipolo están formados por una o varias antenas dipolo y splitters de potencia. Suelen ser antenas omnidireccionales o excéntricas.

Las antenas yagi y los sistemas de antenas yagi están formados por una o varias antenas yagi y splitters de potencia. Estas antenas son siempre direccionales. Las antenas yagi de polarización cruzada son un tipo especial que combina dos antenas en fase de cuarto de onda con polarización ortogonal y alimentación independiente en el mismo brazo. Este tipo de antena se utiliza en aplicaciones que requieren diversidad de polarización o con modo de polarización circular cuando se combinan dos antenas yagi con un splitter de potencia.

Las antenas omnidireccionales pueden ser de media onda alimentadas por el extremo, colineales o de polarización horizontal. Estas antenas radian en todas las direcciones por igual.

Las antenas portátiles suelen ser antenas de cuarto de onda flexibles con métodos de alimentación específicos para garantizar una adaptación de impedancia adecuada con equipos de radio portátiles de tamaño reducido.

Propagación de la señal

Las ondas de radio se propagan principalmente en línea recta, aunque también se pueden producir fenómenos de curvatura, reflexión y difracción. Por lo general, las ondas de radio se propagan simultáneamente de diversos modos y por diferentes trayectos. Esta propagación multitrayecto provoca cierta inestabilidad en la señal como una función del tiempo, porque supone la adición de múltiples señales entrantes que tienen fases diferentes. Esto también explica porqué un pequeño desplazamiento físico de la antena puede influir en la potencia nominal de la señal.

El horizonte radioeléctrico se encuentra aproximadamente un 15% más lejos que el horizonte óptico debido a la tendencia de las ondas de radio a curvarse.

Red radioeléctrica

Para saber si el lado receptor del enlace radioeléctrico dispondrá de potencia y margen suficientes después de la propagación es necesario calcular el balance del enlace radioeléctrico. En estos cálculos todo se expresa en dB, con valor positivo o negativo, y se suma. Los parámetros de cálculo del balance radioeléctrico incluyen la distancia, la frecuencia, el terreno, la altura de la antena, la potencia de salida del transmisor, la sensibilidad del receptor, la pérdida de la línea de alimentación, la ganancia de la antena y la pérdida debida a la propagación. El cálculo del balance del enlace radioeléctrico da siempre el mismo resultado en ambas direcciones.

La cobertura de la red radioeléctrica se puede mejorar utilizando repetidores, que se pueden instalar en puntos adecuados e interconectar para ampliar el área de cobertura.

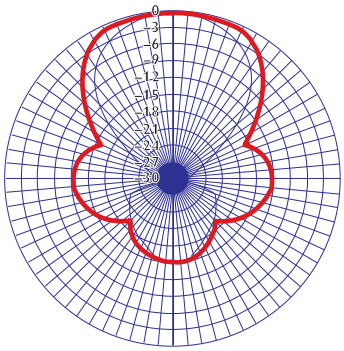


Diagrama
de atenuación de una antena yagi

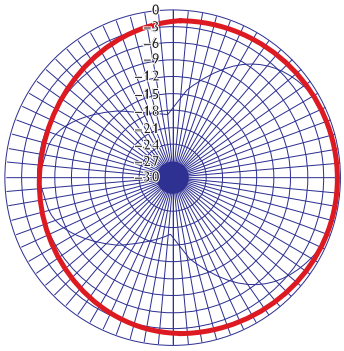


Diagrama
de atenuación de un dipolo

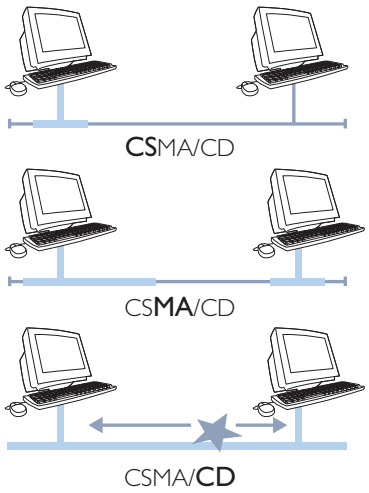
Ethernet industrial

Ethernet es un estándar de transmisión de datos que tiene ya tras de sí una larga historia y que constituye la base de la gran mayoría de las redes instaladas en todo el mundo. Pese a las numerosas voces que a lo largo de los años han pronosticado su desaparición, se sigue desarrollando para ofrecer a los usuarios las propiedades que éstos solicitan. Además, recientemente ha ido ganando aceptación en el sector industrial.

IEEE 802.3 Ethernet

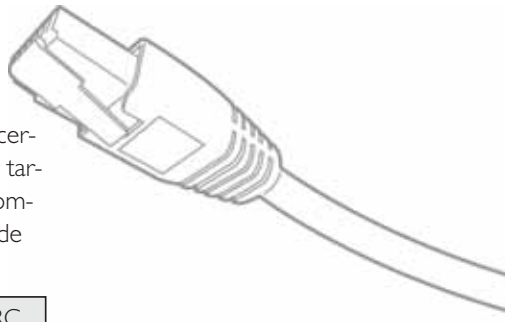
Métodos de acceso

Para que dos o más partes puedan comunicarse es necesario disponer de un conjunto de reglas. Es algo que se aplica a todo, pero muy especialmente a la transmisión de datos. El modo en que los datos se transmiten por la línea se conoce como método de acceso, y el que originalmente utilizaba Ethernet recibió el nombre de CSMA/CD, que significa: **C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **D**etect (protocolo de acceso múltiple con detección de portadora y detección de colisiones). Con todo es importante señalar que Ethernet utiliza dos métodos de acceso: acceso constante o CSMA/CD. Además, aunque CSMA/CD es una referencia común en los manuales, hoy día ya no se utiliza tanto como antes. Sin embargo, por motivos históricos hemos decidido incluir aquí una breve descripción de sus componentes:



- **C**arrier **S**ense (Detección de portadora). Significa que cada unidad individual, antes de enviar datos, debe comprobar si hay alguien más utilizando la red. Si es así, debe esperar para poder transmitir los datos.
- **M**ultiple **A**ccess (Acceso múltiple). Hace referencia a que cualquier dispositivo puede utilizar la red, pero no de manera simultánea.
- **C**ollision **D**etect (Detección de colisiones). Indica que si dos o más unidades transmiten datos simultáneamente, es preciso detectarlo. Cuando se detecta una colisión, se envía una señal de colisión y todas las partes involucradas interrumpen la transmisión. A continuación esperan durante un periodo de tiempo aleatorio antes de volver a intentarlo, lo cual reduce al mínimo los riesgos de que todas las unidades reanuden la transmisión al mismo tiempo. Naturalmente, las colisiones ralentizan el tráfico en el sistema. Las redes con un tráfico muy intenso sufren muchas colisiones, provocando un aumento aún mayor del tráfico, lo que a su vez provoca más colisiones, y así sucesivamente. Algunos equipos tienen pilotos LED que muestran las colisiones, lo que permite comprobar fácilmente la carga de la red. La ventaja de la red CSMA/CD es que todos los equipos pueden comenzar a transmitir en cualquier momento, a diferencia de los sistemas con interrogación o las redes en anillo, en los que la transmisión está sujeta a un control muy estricto.

Direcciones y paquetes en Ethernet



Todo el hardware de Ethernet tiene asignada una dirección única que identifica a cada nodo de la red. Programada en el dispositivo, por ejemplo una tarjeta adaptadora de red, por el fabricante, no se puede modificar mediante software ni tampoco puede hacerlo el usuario, lo que en nuestro ejemplo significa que no hay (o no debería haber) dos tarjetas adaptadoras de red con la misma dirección. Esta dirección recibe a menudo el nombre de dirección MAC (**M**edia **A**ccess **C**ontrol Address, es decir, dirección de control de acceso al medio).

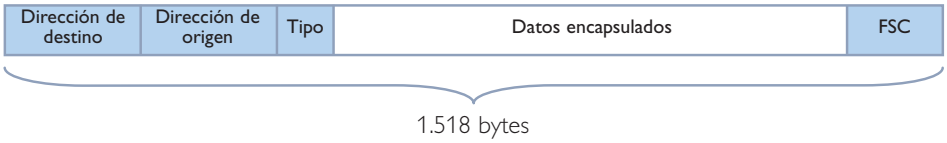
Preámbulo 8 bytes	Dirección de destino 6 bytes	Dirección de origen 6 bytes	Tipo 2 bytes	Datos 46 – 1.500 bytes	CRC 4 bytes

Por su parte, el paquete Ethernet contiene la información siguiente:

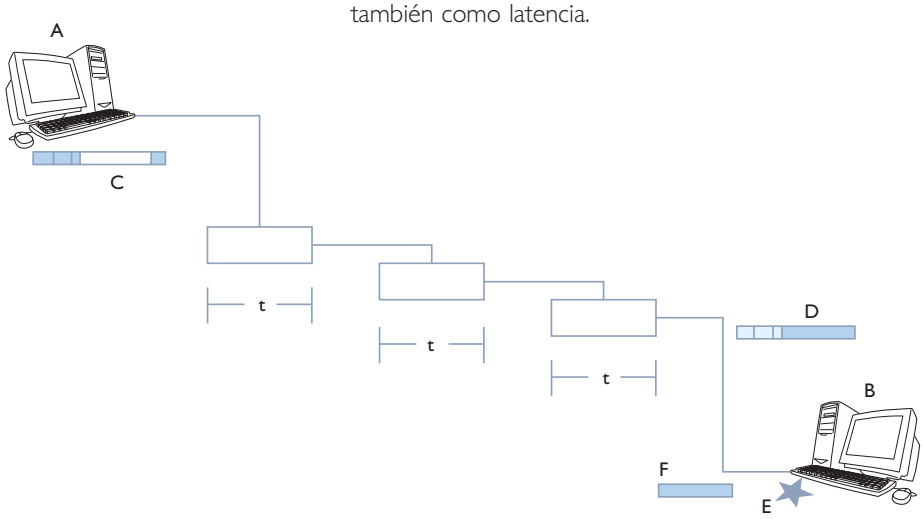
- **Preámbulo.** Es un campo de 64 bits (8 bytes) que contiene un esquema de sincronización formado por unos y ceros alternos y que acaba con dos unos consecutivos. Una vez finalizada la sincronización, el preámbulo se utiliza para localizar el primer bit del paquete. La tarjeta de interfaz LAN es la responsable de generar el preámbulo.
- **Dirección de destino.** Es un campo de 48 bits (6 bytes) que especifica la estación o estaciones a las que hay que enviar el paquete. Cada estación de la red examina este campo para saber si el paquete le está o no destinado.
- **Dirección de origen.** Es un campo de 48 bits (6 bytes) que contiene la dirección única de la estación que transmite el paquete.
- **Tipo.** Es un campo de 16 bits (2 bytes) que identifica el protocolo de capa superior asociado al paquete. Se interpreta en la capa de enlace de datos.
- **Datos.** Este campo puede contener entre 46 y 1.500 bytes. Cada byte (campo de 8 bits) puede incluir cualquier secuencia arbitraria de valores. El campo datos es la información (o paquete) que se recibe de la capa 3 (capa de red). A continuación, la capa 2 divide en tramas de información de 46 a 1.500 bytes los datos (o el paquete) recibido de la capa 3.
- **CRC.** El campo Cyclic Redundancy Check (CRC, comprobación por redundancia cíclica) es un campo de 32 bits de comprobación de errores y se genera a partir de los campos de dirección de destino, tipo y datos.

Dominio de colisiones

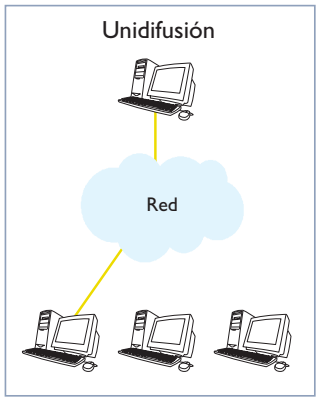
Un dominio de colisiones es un segmento en el que el equipo conectado debe poder detectar y gestionar las colisiones (que se producen cuando varios dispositivos transmiten datos simultáneamente). Los datos que colisionan no desaparecen de manera automática, sino que CSMA/CD se asegura de que se retransmitan. El número de intentos de retransmisión puede limitarse a 16, lo que significa que los datos solamente se perderán después del intento 16, algo que, por otro lado, resulta bastante habitual en las redes Ethernet muy sobrecargadas y con tantos intentos de retransmisión configurados.

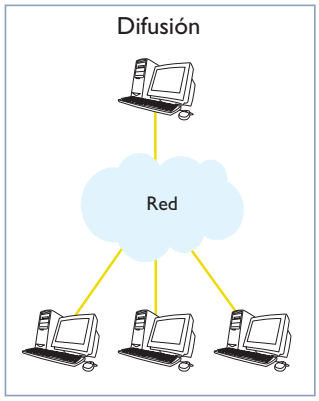


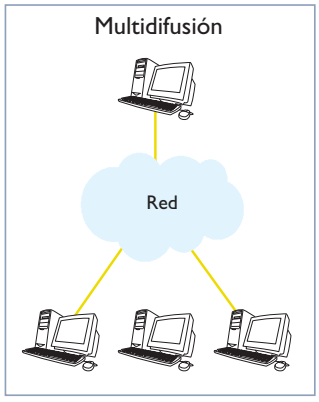
Básicamente, el paquete Ethernet está formado por 1.518 bytes, aunque si se utiliza VLAN se añaden 4 bytes, lo que hace un total de 1.522 bytes. Esta información, junto con la velocidad de la red, son los dos prerrequisitos indispensables para saber con qué rapidez llegará el mensaje a los dispositivos más remotos de la red. Bajo ninguna circunstancia se puede construir un dominio de colisiones de tal modo que el dispositivo emisor sea incapaz de identificar una colisión antes de saber con certeza que el paquete ha llegado a su receptor. La propagación máxima en el dominio de colisiones viene determinada por la red y los equipos instalados, puesto que todos los equipos añaden un retraso, conocido también como latencia.



- Supongamos que **A** intenta enviar un paquete a **B**.
- La red incluye una cantidad determinada de equipos que tienen un retraso interno (**t**).
- **A** vacía constantemente su búfer de envío si no se detecta ninguna colisión.
- Se produce entonces una colisión en el nodo más remoto de la red (**E**).
- No se reciben todos los datos (**D**) y, por tanto, (**B**) no puede interpretarlos.
- Como resultado, se envía la señal de colisión (**F**) al transmisor (**A**).
- Sin embargo, si el dominio es demasiado grande la señal de colisión no llegará a (**A**) antes de que éste vacíe el búfer de envío, haciendo imposible retransmitir el paquete.







Redes IP

Protocolo de Internet (IP)

IP (Internet Protocol) es un protocolo diseñado específicamente para interconectar los equipos de una red o de varias redes. Cuando se elaboró la especificación, se dio por supuesto que constantemente aparecerían nuevas tecnologías y métodos de transmisión. Por eso se decidió hacer de IP un estándar abierto que, ante todo, fuera independiente de la red y del medio subyacentes. TCP/IP es una familia de protocolos que abarca muchas capas diferentes del modelo OSI.

Métodos de direccionamiento

Gran parte de la información que circula por la red va de un único emisor a un único receptor. Es algo totalmente natural en la mayoría de los casos, por ejemplo, en la comunicación entre un PLC y un dispositivo de E/S. Este tipo de transmisión se conoce como unidifusión.

Justamente lo contrario de la unidifusión es la «difusión», que es como se transmiten, por ejemplo, las señales de radio y televisión: un emisor y muchos receptores. La difusión implica el envío de la información a todos, y se utiliza en algunas redes de ordenadores muy cercanas. Sin embargo, esta técnica no se puede utilizar en Internet, porque sobrecargaría la red.

Por último, la multidifusión es una técnica a medio cambio entre la unidifusión y la difusión. En este caso, la información no se envía indiscriminadamente a todo el mundo como ocurre en la difusión, pero, al contrario de la unidifusión, puede ir dirigida a muchos destinatarios. La técnica de multidifusión permite construir redes de distribución, adecuadas para controlar las transmisiones de vídeo y televisión por Internet, es decir, transmisiones con un único emisor y muchos receptores. Sin duda, la multidifusión brindará nuevas oportunidades de desarrollo para Internet, y evitará que se colapse por sobrecarga.

Byte	1	2	3	4
	192.	168.	3.	23

Direcciones de red

Antes de entrar a describir cómo se construye una dirección IP, conviene aclarar algunos conceptos:

- La dirección IP consta de cuatro bytes.
- Cada byte está formado por 8 bits de datos. Por ejemplo, 11000000, que corresponde al valor decimal 192. Fíjese en el byte 1 del ejemplo.
- Por su parte, las direcciones se asignan en diferentes clases (A, B, C, D y E), siendo la clase un intervalo de dirección. Actualmente existen cinco clases de direcciones, de las cuales las tres primeras (A-C) se utilizan para diferentes tipos de redes en las que la dirección IP está dividida en una parte de red y una parte de ordenador. Además existen las clases D y E. La clase D es para direcciones multidifusión, y la clase E está reservada para usos futuros.
- Las direcciones IP en redes de clase A, B y C se dividen en dos partes, una parte de red y una parte de ordenador.

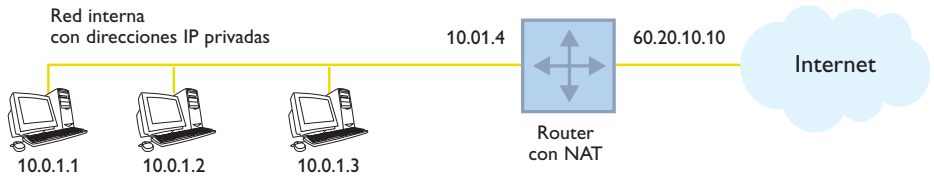
Clase	Primer byte	Intervalo de dirección
A	**0**xxx xxxx	**0**.0.0.0 hasta **127**.255.255.255
B	**10**xx xxxx	**128**.0.0.0 hasta **191**.255.255.255
C	**110**x xxxx	**192**.0.0.0 hasta **223**.255.255.255
D	**1110** xxxx	**224**.0.0.0 hasta **239**.255.255.255
E	**1111** xxxx	**240**.0.0.0 hasta **247**.255.255.255

Las redes A, B y C se diferencian en el número de bits utilizados para la identificación de la red y del dispositivo:
La identidad de red de clase A comprende 8 bits (1 byte); la de clase B, 16 bits, y la de clase C, 24 bits. Ello permite asignar direcciones a un número distinto de dispositivos en sus respectivas redes (consulte también la división en subred que se muestra a continuación).

Clase					Valor decimal en el byte 1	Número máx. de dispositivos en la red
A	Red	Ordenador	Ordenador	Ordenador	de 0 a 127	16 777 215
B	Red	Red	Ordenador	Ordenador	de 128 a 191	65 535
C	Red	Red	Red	Ordenador	de 192 a 223	255

Direcciones públicas y privadas

Pueden darse casos en los que no se pueda o no se desee utilizar direcciones IP públicas en la red interna. En esos casos se pueden utilizar direcciones IP privadas (RFC1918). Sin embargo, como las direcciones IP privadas no permiten conectarse a Internet, hay que utilizar la **N**etwork **A**ddress **T**ranslation (NAT, traducción de dirección de red).



Un router o un firewall con soporte para NAT traduce las direcciones privadas en direcciones públicas:
Cuando el ordenador que tiene la dirección 10.0.1.2 tiene que acceder a Internet se direcciona a 10.0.1.4, que es la «pasarela predeterminada» o de salida. Cuando los datos de la dirección 10.0.1.2 pasan por el router, NAT traduce la dirección IP interna 10.0.1.2 a 60.20.10.10, esto es, la dirección IP «de puertas afuera». Así es como se comunica un equipo con una dirección IP interna con otros ordenadores a través de Internet. Da igual si al mismo tiempo se establece una comunicación desde otra dirección IP interna, ya que el router gestiona a qué dirección IP interna corresponde cada sesión y se asegura de que cada ordenador de la red interna reciba los datos correctos.

La **I**nternet **A**ssigned **N**umbers **A**uthority (IANA, autoridad de números asignados de Internet) ha reservado los siguientes tres bloques de direcciones IP para direcciones IP de redes privadas:
10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

Ipv4 e Ipv6

IPv6 es la versión 6 del protocolo IP, creada a finales de la década de 1990 para sustituir a la anterior, Ipv4 (versión 4 del protocolo), principalmente porque las direcciones IP están empezando a terminarse. La principal diferencia entre IPv6 e IPv4 radica en que la longitud de la dirección se ha incrementado de 32 a 128 bits, lo que significa que el número de direcciones posibles ha pasado de 4.000 millones a una cifra realmente astronómica.

Cabecera de Ipv6

Dirección de origen de 128 bits		
Longitud del paquete	Siguiente cabecera	Límite de saltos
Dirección de origen de 128 bits		
Dirección de destino de 128 bits		

División de la subred

Las redes locales con más de unos cientos de dispositivos conectados son poco habituales. Dejar que este tipo de redes lleve su propia clase A o B (más de 16 millones de redes con 65.000 dispositivos posibles en cada red) supone un desperdicio tremendo de direcciones disponibles. Para evitarlo, la mayoría de estas clases se dividen en una **subred**, en la que una parte de la identidad del dispositivo se utiliza como una especie de dirección de red. La división se hace empleando una parte de la identidad del dispositivo, justamente en la «frontera» con la dirección de red, y la identidad del dispositivo «se mueve», de manera que el número de identidades de red disponibles aumente, al tiempo que disminuye el número de dispositivos de la subred. Para poder hacerlo se utiliza una **máscara de red** en la que los bits que pertenecen a la parte de red se configuran a uno (mientras que los bits del ordenador se configuran a cero).

Entre las ventajas de este procedimiento se encuentran las siguientes: las redes más pequeñas son más fáciles de administrar, el tráfico de datos en la subred es más reducido y configurar y mantener la red física resulta más sencillo (por ejemplo, se pueden montar diferentes subredes en las distintas plantas de un edificio).

Las clases A, B y C tienen las máscaras de red estándar (es decir, sin subred) siguientes:

Clase de dirección	Máscara de red	Valor binario Byte 1	Valor binario Byte 2	Valor binario Byte 3	Valor binario Byte 4
A	255.0.0.0	11111111	00000000	00000000	00000000
B	255.255.0.0	11111111	11111111	00000000	00000000
C	255.255.255.0	11111111	11111111	11111111	00000000

Como decíamos antes, una dirección IP de clase B consta de dos partes del mismo tamaño 2 bytes para la identidad de red y otros 2 bytes para la identidad de dispositivo que se pueden representar como N.N.D.D, donde N es cada byte de identidad de red y D cada byte de identidad de dispositivo. Por consiguiente, la máscara de red resultante es 255.255.0.0.

Si se utiliza el tercer byte completo para definir la subred en lugar de la identidad de dispositivo, la dirección se puede interpretar como N.N.N.E, en cuyo caso la máscara de red sería 255.255.255.0.

De ello se deriva que tenemos 254 redes de tipo C con 254 ordenadores en cada una (la primera y la última direcciones de las partes de red y ordenador están reservadas).

En principio, cualquiera de los bits de un byte se puede utilizar para definir una subred, pero normalmente se destinan a este fin los más altos, porque de este modo se simplifica mucho la gestión de la red.

Si, por ejemplo, los primeros tres bits de una dirección C se utilizan para direcciones de subred, la red C podría dividirse en 6 subredes (consulte las combinaciones de redes posibles más abajo). Dos combinaciones de bits de la identidad de dispositivo (11111 y 00000) se reservan para difusión e identidad de red, que es la razón por la que el número de direcciones disponibles es 30 en cada una de las redes.

Máscara de red	Máscara de red de tipo C	3 primeros bits en la máscara de red de tipo C	Otros bits en la máscara de red de tipo C	Sub-red	Número de identidades de dispositivo
255.255.32.0	32	001	00000	1	30
255.255.64.0	64	010	00000	2	30
255.255.96.0	96	011	00000	3	30
255.255.128.0	128	100	00000	4	30
255.255.160.0	160	101	00000	5	30
255.255.192.0	192	110	00000	6	30

Puertos

Una aplicación recibe los datos por un número de puerto especial que identifica la comunicación con esa aplicación.

Por ejemplo, un ordenador puede ser un servidor web, un servidor de correo electrónico y un servidor DNS al mismo tiempo. Para que el tráfico de las diferentes aplicaciones no tenga colisiones, es preciso dividirlo, y se hace predefiniendo el número de puerto a la aplicación. Del 1 al 1024 son números de puerto conocidos y no deben utilizarlos aplicaciones distintas de las especificadas.

Son ejemplos de números de puerto conocidos:

21	ftp	Transferencia de archivos
23	Telnet	Telnet
25	smtp	Correo electrónico. Transferencia de correo simple
80	http	World Wide Web

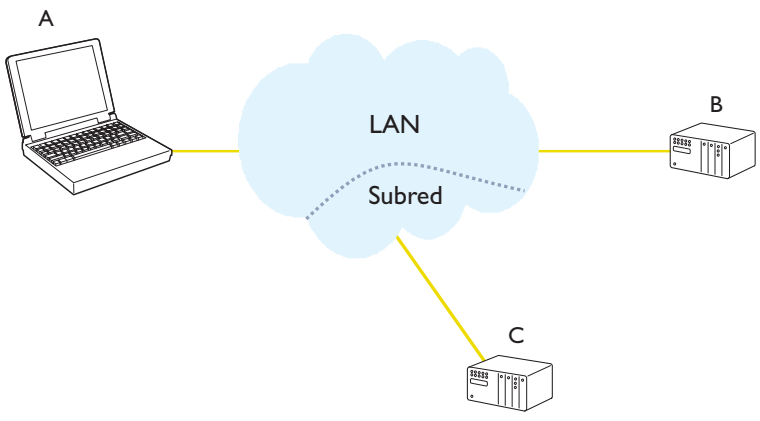
La lista completa de números de puerto figura en www.iana.org/assignments/port-numbers

Dirección MAC

Abreviatura de Media Access Control address (MAC, dirección de control de acceso al medio), es una dirección de hardware que identifica de forma exclusiva a cada nodo de la red. Programada en el dispositivo, por ejemplo una tarjeta adaptadora de red, por el fabricante, no se puede modificar mediante software ni tampoco puede hacerlo el usuario, lo que significa que no hay (o no debería haber) dos tarjetas adaptadoras de red con la misma dirección MAC.

ARP

Los ordenadores u otro tipo de hardware conectados a una red TCP/IP tienen como mínimo una dirección IP. La dirección IP también se conoce como la dirección lógica, ya



que suele estar implementada en el software y se puede cambiar dependiendo de la ubicación física del hardware en la red. Los dispositivos también tienen una dirección física, que en Ethernet se denomina dirección MAC, única para cada componente de hardware conectado.

Así, dos equipos (A) y (B) que utilicen TCP/IP para comunicarse por Ethernet deben tener registrada la dirección MAC de la contraparte, pues toda la comunicación por Ethernet se basa en las direcciones MAC.

Debido a ello, los dispositivos A y B tienen su propia tabla ARP de direcciones IP y de direcciones MAC asociadas.

El **A**ddress **R**esolution **P**rotocol (ARP, protocolo de resolución de direcciones) actualiza dinámicamente las tablas ARP, de modo que la correspondencia entre la dirección IP y la dirección MAC siempre se conozca.

- Supongamos que el ordenador (A) quiere comunicarse con el PLC (B). El ordenador (A) ya conoce la dirección IP (de B) (por ejemplo, porque la ha configurado manualmente el operador) pero desconoce la dirección MAC (de B). Los dispositivos no podrán comunicarse hasta que (A) conozca la dirección MAC (de B).
- A descubre que B se encuentra en la misma red comparando la dirección IP de destino y la máscara de red.
- A envía una petición ARP en un mensaje de difusión. La petición contiene las direcciones IP y MAC (de A) y la dirección IP de B.
- Todas las unidades de la red comprenden el mensaje, pero sólo B reconoce su dirección IP y envía una respuesta ARP que contiene su propia dirección MAC.
- Como resultado, A puede actualizar su tabla ARP, de manera que contenga también la dirección MAC de B.

Punto a punto (PPP)

En ocasiones se hace necesario conectarse y comunicarse utilizando el protocolo TCP/IP por una conexión serie, concretamente en las conexiones a Internet por módem o a una red de área local. La forma que adopta la comunicación depende de la aplicación, pero en todas ellas se utiliza el **P**oint to **P**oint **P**rotocol (PPP, protocolo punto a punto) que es sin duda el protocolo de enlace más utilizado para la conexión remota de ordenadores a una red. Son ejemplos de comunicaciones serie los módems telefónicos, los módems con línea dedicada propia, los módems RDSI y GSM, los módems de radio y los de corto alcance.

Seguridad (CHAP y PAP)

El protocolo PPP se utiliza a menudo en las conexiones punto a punto remotas, ya sea por línea conmutada, RDSI o línea dedicada. Generalmente es preciso garantizar cierta seguridad entre las partes en comunicación. Pues bien, PPP admite dos métodos de verificación del usuario: **P**assword **A**uthentication **P**rotocol (PAP, protocolo de autenticación de contraseña) y **C**hallenge **H**andshake **A**uthentication **P**rotocol (CHAP, protocolo de autenticación por reto) para este propósito. No obstante, ni la autenticación ni la verificación de mensajes son obligatorias en PPP, por lo que las partes tienen libertad para comunicarse sin identificación o sin negociar qué protocolo van a utilizar. En cualquier caso, lo mejor es elegir CHAP. De hecho, PAP sólo se suele seleccionar en aquellos casos en que una de las partes no soporta CHAP.

PAP funciona de manera muy similar al acceso desde un terminal, indicando el nombre de usuario y la contraseña. La autenticación se realiza durante el establecimiento de la conexión, nunca durante la comunicación.

- El procedimiento PAP se inicia cuando una de las partes envía una petición de autenticación con un nombre y una contraseña. El paquete se reenvía hasta que la contraparte responde.
- Si el nombre y la contraseña se aceptan, el receptor contesta con una confirmación de la autenticación. En caso contrario, el receptor envía una respuesta de no confirmación de la autenticación y desconecta.

Sin embargo, como el nombre y la contraseña se envían como texto sin formato por el enlace, PAP es un método de autenticación relativamente vulnerable. En efecto, la contraseña puede resultar interceptada con facilidad mediante una simple escucha y además no existe protección alguna contra ataques por prueba y error repetidos.

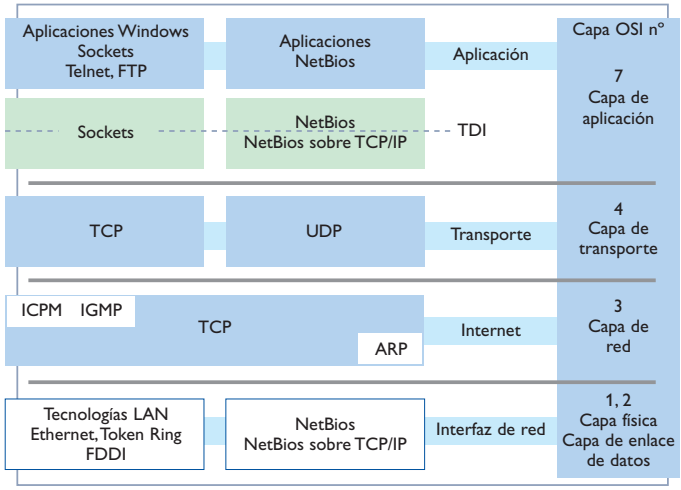
CHAP es un protocolo mucho más seguro que PAP

CHAP utiliza una contraseña cifrada en un procedimiento en tres pasos. Además, parte de la autenticación tiene lugar una vez que la conexión está establecida, y luego se puede repetir en cualquier momento. La idea de la repetición periódica es limitar el tiempo que el sistema está abierto a los ataques. Siempre es el autenticador (el receptor) el que determina la frecuencia con la que se realiza la autenticación. Los tres pasos de la autenticación son los siguientes:

- Cuando se establece el enlace, una de las partes (el autenticador) envía un reto a su igual.
- El igual calcula un valor cifrado basado en el reto y en su contraseña, tras lo cual remite el valor cifrado al autenticador.
- El autenticador realiza un cálculo equivalente (conoce el reto y la contraseña de su igual) y compara el valor resultante con el que ha recibido de la otra parte. Si el valor es idéntico, confirma la autenticación; en caso contrario, desconecta.

TCP/IP y UDP/IP

En el modelo OSI, cada capa es responsable de los datos que circulan por ella. La capa de transporte es la responsable de transferir los datos, para lo cual puede utilizar uno de los dos protocolos disponibles: TCP o UDP.



UDP

El **U**ser **D**atagram **P**rotocol (UDP, protocolo de datagrama de usuario) se suele clasificar entre los protocolos no orientados a conexión, lo que significa que se pueden enviar datos sin importar si el receptor existe o no. Además, el receptor no envía al emisor acuse de recibo de los datos. Como los datos se transmiten sin que haya una conexión establecida, la transferencia es más eficaz y, por lo general, más rápida. En consecuencia, UDP se utiliza en aplicaciones que requieren un uso eficaz del ancho de banda y en las que se pueden retransmitir los datos perdidos en caso necesario.

De hecho, el protocolo UDP se puede comparar con el envío de una carta: los datos se introducen en un sobre con una dirección. Una vez enviada la carta, lo único que puede hacer el emisor es esperar que la oficina de correos la entregue a su destinatario. Otra característica reseñable de UDP es la posibilidad de enviar mensajes de «difusión» y «multidifusión», es decir, un mensaje con múltiples destinatarios. De hecho, esta es la principal ventaja de utilizar UDP.

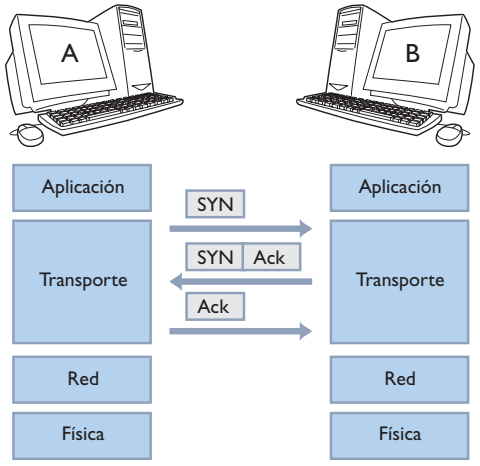
TCP

El **T**ransmission **C**ontrol **P**rotocol (TCP, protocolo de control de transmisión) es un protocolo orientado a conexión, lo que significa que la conexión se establece antes de que los dispositivos empiecen a intercambiar datos. TCP tiene una responsabilidad mayor en los datos transmitidos que UDP, puesto que el receptor envía un acuse de recibo (ACK) por cada paquete de datos enviado. Si el emisor no recibe el ACK, vuelve a transmitir el paquete, lo que garantiza su recepción.

Otra característica de TCP es que este protocolo mantiene un control sobre la secuencia y el flujo cuando se transmiten grandes cantidades de datos. En efecto, los paquetes TCP pueden llegar al receptor en un orden distinto al de envío, pero TCP les asigna un número de secuencia que garantiza que se ordenarán adecuadamente a su llegada a destino. Debido a la necesidad de establecer la conexión y de acusar recibo de los datos transmitidos, TCP tarda más que UDP en enviar los datos y, además, consume más ancho de banda.

Cómo se establece la conexión TCP

Las conexiones TCP se establecen mediante un procedimiento de negociación que incluye tres pasos:



- El cliente A envía una petición de conexión con el bit SYN activado. De este modo, el cliente puede sincronizar un número de secuencia con el servidor (B).
- El servidor (B) envía un acuse de recibo (ACK) al cliente con su bit SYN activado y, simultáneamente, sincroniza su número de secuencia con el cliente.
- Por último, el cliente acusa recibo (ACK).

La transmisión puede incluir uno o más bytes, que están numerados y de los que se envía acuse de recibo.

La conexión se interrumpe cuando el cliente (A) comprueba el paquete TCP local y toda la información se ha transmitido y su llegada ha sido confirmada. A continuación se envía un paquete TCP con el bit FIN activado. El servidor (B) acusa recibo, pero continúa enviando datos si la aplicación así lo requiere. Cuando la transmisión finaliza, el servidor (B) envía un paquete TCP con el bit FIN activado.

Cómo construir una red

Dispositivos de la red

Repetidores

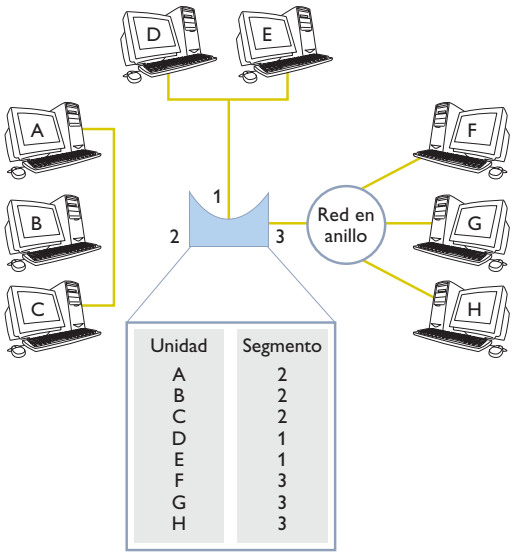
Un repetidor es una especie de amplificador; no es un dispositivo inteligente y se limita a recrear las señales. En efecto, las señales se van atenuando en función de la longitud del medio y de la frecuencia de la señal, lo que limita el alcance de la red. El repetidor permite aumentar la longitud del medio, pues este dispositivo recrea la señal devolviéndole la fuerza y el aspecto iniciales. El repetidor trabaja dentro del mismo dominio de colisiones (HDPX CSMA/CD) y presenta una latencia añadida que impide instalar en el mismo segmento un número ilimitado de ellos.

Bridge

El bridge separa dos o más dominios de colisiones y se puede utilizar para conectar topologías diferentes. El bridge escucha y registra las correspondencias entre direcciones y segmentos, de tal modo que sabe a qué segmento están conectados los distintos dispositivos.

Este dispositivo se utiliza, por ejemplo para conectar una red Ethernet a otra en anillo. Los bridges suelen trabajar de manera selectiva, lo que significa que filtran las direcciones de manera que los datos lleguen únicamente a la dirección de destino (por ejemplo, los dispositivos A y B sólo se comunican en el segmento 2). Así, la red está dividida y el tráfico interno no sobrecarga otros segmentos.

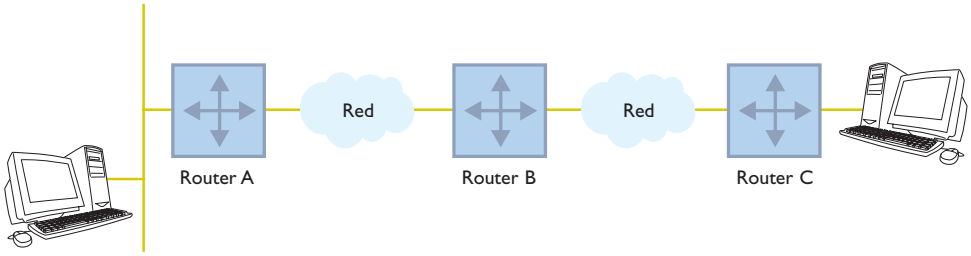
El bridge trabaja en el sistema de encaminamiento de la capa MAC, basándose únicamente en su dirección física. En cambio, el router toma las decisiones sobre la base de las direcciones de la capa 3.



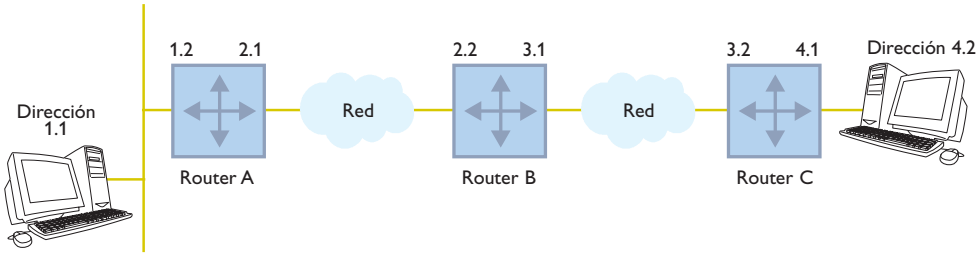
Unidad	Segmento
A	2
B	2
C	2
D	1
E	1
F	3
G	3
H	3

Router

La palabra «route» significa seleccionar o encontrar el trayecto adecuado. Un router es un dispositivo (en algunos casos una aplicación de software de un ordenador) que determina por dónde hay que enviar un paquete en su camino hacia el destino final (desde el punto de vista de una red LAN, el router es el destino final). Por consiguiente, el router es un dispositivo de red que conecta dos o más redes separadas lógicamente. Sin embargo, no las conecta a ciegas, sino que actúa en cierto modo como un switch de paquetes para interconectar redes locales a corta o larga distancia. Además de los equipos instalados en redes separadas, la red puede utilizar diferentes topologías y normas.



Como todos los dispositivos tienen una dirección única, el equipo emisor siempre puede dirigirse a un receptor concreto de la misma red o de otra diferente. Cuando el receptor es un dispositivo de otra red, los datos se encaminan de la manera adecuada mediante una conexión lógica entre las redes. La información necesaria para ello se reúne en una tabla de encaminamiento que define el trayecto y opciones alternativas de conexión.



Para el ejemplo ilustrativo hemos adoptado una técnica de direccionamiento simplificada. Las direcciones de red son 1, 2, 3 ó 4. Los dispositivos que se encuentran en la misma red tienen las direcciones 1.1, 1.2, etc.

Supongamos que el ordenador que tiene asignada la dirección 1.1 quiere comunicarse con el ordenador con dirección 4.2. El router A recibe un paquete dirigido a 4.2, detecta que la dirección pertenece a otra red y lo encamina hacia el siguiente punto de la red, en este caso a 2.1 y luego a 2.2. Lo mismo ocurre entre los routers B y C. Finalmente, el paquete llega al router C, desde donde se transfiere a la red 4, al ordenador que tiene asignada la dirección 4.2.

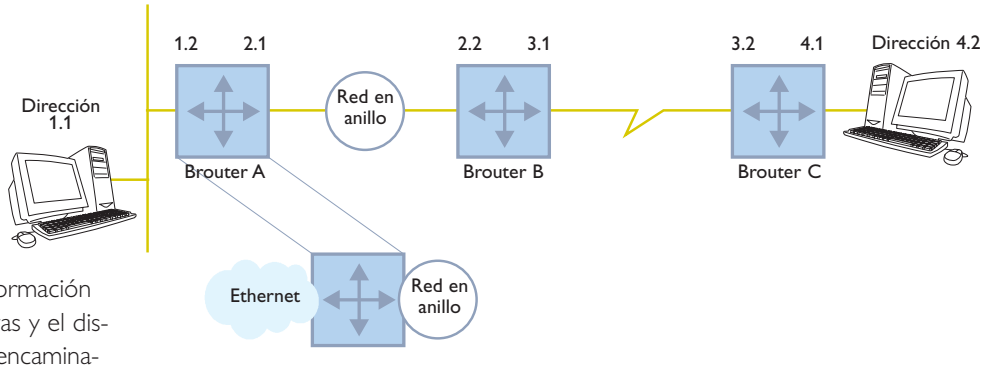
Además de encaminar el tráfico, también existe la posibilidad de controlarlo y filtrarlo. La tabla de encaminamiento que recoge la ubicación de los diferentes equipos y redes puede ser dinámica o estática. Las tablas de encaminamiento dinámicas se actualizan automáticamente a partir de la estructura que tienen a su alrededor.

El modo en que debe encaminarse el tráfico se controla con un protocolo de encaminamiento, por ejemplo, **R**outing **I**nformation **P**rotocol (RIP, protocolo de información de encaminamiento), o bien **O**pen **S**hortest **P**ath **F**irst (OSPF) un protocolo que abre primero el camino más corto.

Brouter

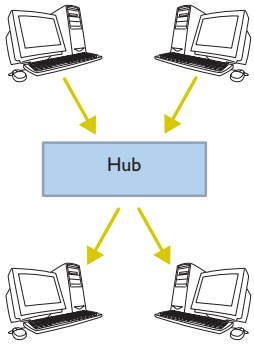
De los numerosos estándares que ofrece el mercado, los más comunes son Ethernet, Token Ring y FDDI. Aunque cada uno tiene sus propias técnicas y formatos de comunicación, el direccionamiento es el mismo en todos ellos y está normalizado por el IEEE.

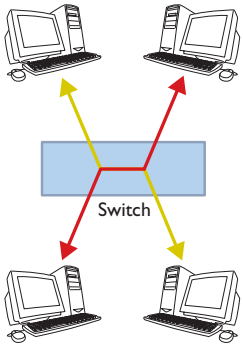
Un brouter es un dispositivo que combina las funciones de bridge y router. De hecho, muchos de los routers actuales son en realidad brouters. Así, cuando el dispositivo tiene que transmitir el mismo protocolo dentro una LAN, o a otra LAN, entra en acción la función de bridge. En cambio, si el PC está conectado a una red WAN (**W**ide **A**rea **N**etwork), se requiere más información sobre las conexiones alternativas y el dispositivo necesita una tabla de encaminamiento. En este caso, se combinan las funciones de router y bridge.



Hub

El hub o concentrador es un dispositivo de red que hace las veces de conexión central en una red, como si se tratara de una conexión en estrella. Los datos que llegan por un puerto se envían a todos los demás, con independencia de cuál de ellos sea el receptor. El hub fue el dispositivo de red que propició el éxito del estándar de cableado 10basteT. En efecto, brindó oportunidades de creación de redes totalmente nuevas, con equipos centrales y puntos de conexión en cada centro de trabajo. Existen dos tipos de hubs: activos y pasivos. El hub pasivo conecta segmentos de red sin amplificar la señal, mientras que el hub activo ofrece además amplificación de la señal.





Switch

El switch se parece al hub en que también es el punto de conexión central de la red. La diferencia estriba en que el switch mantiene un registro de los dispositivos conectados y de sus puertos correspondientes. Así, cuando se envían datos a un dispositivo de la red, el switch comprueba la dirección del receptor y transmite los datos únicamente al puerto al que está conectado el dispositivo (red con conmutación). De este modo la red no se sobrecarga con tráfico innecesario. Otra de sus ventajas es que aumenta el nivel de seguridad, dado que dificulta el acceso a la información dirigida al ordenador receptor.

Un switch de capa 2 es una especie de bridge.

Un switch de capa 3 es una especie de router.

Por este motivo, en algunos contextos los términos switch, bridge y router se utilizan como sinónimos.

Además, los switches pueden ser de tipo gestionado o no gestionado. La diferencia es que el switch gestionado (supervisable) permite el acceso a sus funciones, normalmente por SNMP (consulte también las páginas 138 a 143).

Gateway

Una gateway es un dispositivo que permite interconectar redes, aunque su función principal consiste en convertir los datos entre diferentes protocolos, por ejemplo AppleTalk y TCP/IP. Además de esta función de conversión, la gateway admite distintos formatos, códigos de caracteres, direcciones, etc.

Firewall

El firewall es un dispositivo o un software especial que sólo permite el paso del tráfico que cumple determinados requisitos, bloqueando el resto. De este modo se garantiza la protección de los usuarios de una red contra el tráfico no deseado. Por lo general, el firewall se instala entre la red local e Internet, aunque también se puede poner en redes internas o en los equipos de acceso a la red. Para determinar qué tráfico debe dejar pasar el firewall se utilizan reglas de diversa complejidad. En realidad, son los requisitos de seguridad definidos en la red los que controlan el cuándo, el dónde y el cómo debe trabajar el firewall. El mercado ofrece una gran diversidad de productos entre los que elegir, desde los que combinan soluciones de hardware y software hasta los firewall «freeware» que se pueden descargar de Internet e instalar en el ordenador.

Hub o switch

¿Por qué es mejor un switch que un hub y cuál es la diferencia entre estos dos productos? Ya hemos indicado que el hub hizo posibles las redes en estrella y que, junto con Ethernet, popularizó los sistemas de cableado estructurado. Sin embargo, el hub no tiene un diseño avanzado; todo lo que se envía a un puerto se transfiere también a los otros puertos. Como resultado, todos los equipos reciben lo que envían los demás, y todos ellos están en el mismo dominio de colisiones.

Por otro lado, el switch es un dispositivo con un grado mayor de inteligencia, gracias a los procesadores o los circuitos integrados especialmente diseñados que lleva. De este modo, puede controlar y procesar los datos recibidos en un puerto. El switch sabe qué equipo está conectado a cada puerto, información que guarda en su memoria de direcciones MAC. Hay dos tipos de switch, los que trabajan en modo «cut-through» y los que lo hacen en modo «store-and-forward». Los primeros examinan la dirección de destino y envían los datos al puerto de destino. Su principal desventaja es que pueden provocar una colisión si el puerto está ocupado con tráfico, provocando la pérdida del paquete más reciente. Como contrapartida, son muy rápidos. Los switches de tipo «store-and-forward» copian el paquete recibido y lo ponen en el búfer antes de localizar el puerto de destino, y además no lo envían hasta que el puerto está libre. De este modo el paquete no se pierde y los datos se pueden priorizar, la red se puede dividir en LAN virtuales, etc.

El cuadro siguiente recoge algunas de las diferencias entre el hub y el switch.

Hub	Switch
Comunicación half dúplex.	Half dúplex o full dúplex (HDX/FDX).
Aumenta el dominio de colisiones.	Segmenta la red.
Toda la red comparte el ancho de banda.	Ancho de banda a medida (sistema de autoaprendizaje).
Desaprovecha el ancho de banda debido a CSMA/CD.	Función «store-and-forward» (control del paquete antes de reenviarlo).
Más rápido que el switch (menos latencia).	Aprende las direcciones MAC (qué hay conectado y dónde).
	Olvida las direcciones antiguas (fin de la temporización en el búfer de direcciones MAC).
	Control de flujo para FDX y HDX.
	Búfer de paquetes en el nivel de puerto.
	QoS, priorización de datos (los datos con prioridad alta se colocan en primer lugar en el búfer de paquetes).
	Red virtual VLAN (interconecta virtualmente puertos específicos).
	Switches con capacidad del orden del Gbit (switches potentes de alta capacidad).

La ventaja que siempre resaltamos es que el switch segmenta la red (Ethernet conmutada), lo que elimina las colisiones.

Diferentes tipos de switches

Existen diferentes switches adaptados a los requisitos de la aplicación y de la instalación. Así, atendiendo al tipo de interfaz, los hay para TX (cobre) y FX (fibra). Además están los switches gestionados y los no gestionados, según ofrezcan o no al operador la posibilidad de comunicarse con ellos y de supervisarlos con SNMP. Por último, los hay para redes en anillo y para redes sincronizadas, que se utilizan para crear redes en anillo con redundancia o en redes que requieren sincronización horaria.

FRNT y el protocolo de árbol de extensión (Spanning Tree)

Las redes complejas que necesitan redundancia deben poderse reconfigurar en caso de fallo.

El switch es el dispositivo que gestiona la reconfiguración, lo que significa que tiene que ser capaz de detectar que se ha producido un error de enlace. Para ello se pueden utilizar diferentes protocolos, entre los que figuran algunas soluciones normalizadas por el IEEE: el **S**panning **T**ree **P**rotocol (STP, protocolo de árbol de extensión) o el **R**apid **S**panning **T**ree **P**rotocol (RSTP, protocolo de árbol de extensión rápido). El primero de ellos, STP, crea una conexión a través de la red al tiempo que elimina los bucles indeseados. Este protocolo garantiza la redundancia manteniendo la estructura de árbol de la red en orden, con algunas conexiones bloqueadas (en modo de espera). Si no se puede llegar a un segmento, la red se vuelve a configurar con el algoritmo de árbol de extensión, que pone en modo activo todas las conexiones que estaban en modo de espera. La reconfiguración de una red STP puede llevar hasta 30 segundos, debido a la necesidad de calcular las nuevas condiciones y de actualizar los switches. Se trata de un cálculo complejo, porque la red no tiene una topología determinada. El protocolo RSTP es una evolución de STP que hace más rápida la reconfiguración (tan solo 5 segundos).

Además de las anteriores, existen soluciones desarrolladas específicamente, como **F**ast **R**ecovery **N**etwork **T**opology (FRNT, topología de red de recuperación rápida), que es la que utilizamos en nuestros modelos de switch R200 para red en anillo y T200 para red con sincronización horaria. FRNT es una solución patentada que reconfigura la red a una velocidad extraordinaria <30 ms, gracias a que los switches conocen la configuración de la red y a que ésta es de topología en anillo. Además, la reconfiguración es un evento controlado, pues el «tráfico libre» se envía entre los dispositivos del anillo para comprobar en qué puntos está activo el enlace. Si se detecta un error, la información se envía inmediatamente al punto central del anillo (ringmaster), que vuelve a configurar la red.

Switch para red en anillo

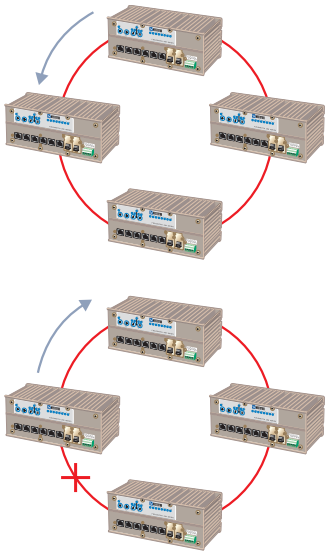
Tenemos dos versiones de switches para red en anillo: una para anillos básicos y otra para anillos puenteados. Todos los modelos incluyen el software de reconfiguración FRNT0 o FRNT1.

FRNT0

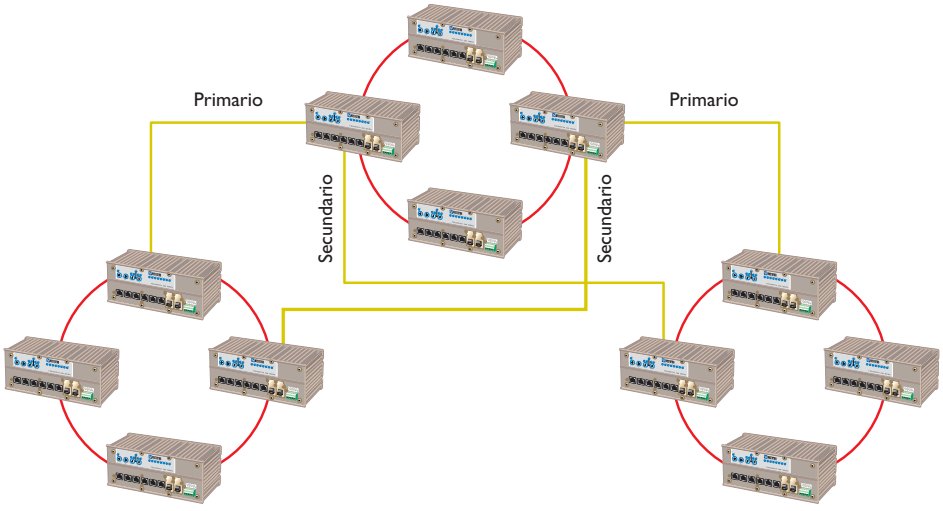
En las redes en anillo el tráfico puede circular en dos direcciones, hacia la derecha o hacia la izquierda. El switch para red en anillo utiliza ambas, eliminando así los errores de red. En efecto, si se produce un error, el switch, que está configurado como punto central, recibe una notificación y vuelve a configurar la red para que todos los equipos se puedan comunicar entre sí.

FRNT1

Algunos switches pueden interconectar varias redes de anillo, lo que refuerza la fiabilidad. Cada anillo incorpora un enlace primario y otro secundario que permiten establecer un puente con otros anillos de la red. Cuando se produce un error en el enlace primario, el punto central recibe la notificación correspondiente. El switch vuelve a configurar la red y conecta el enlace secundario al anillo subyacente. Si el fallo está en un cable, es primordial solucionarlo. Sin embargo, en las redes con redundancia este tipo de fallos solamente se detecta cuando generan una alarma.



FRNT0



FRNT1

Switches con servidor de tiempo

Ethernet no es de diseño determinista, lo que significa que no se puede garantizar el tiempo de transmisión de un paquete de datos de una vez a otra. Como resultado, antes era imposible utilizar Ethernet en aplicaciones de tiempo real, como las de control de subestaciones eléctricas o de maquinaria compleja. Hoy día estas limitaciones han desaparecido. En los sistemas de tiempo real, todos los enlaces deben ser full dúplex y tener el control de flujo (en el nivel Ethernet) desactivado. Además, debe ser posible asignar prioridad a los datos, de manera que los que tengan prioridad alta se coloquen al principio de la cola y se transmitan al receptor de forma prioritaria. En combinación con la función de sincronización horaria, este tipo de switches permite diseñar aplicaciones de tiempo real sobre Ethernet (consulte también las páginas 136 y 137).

Principales fuentes de problemas para las aplicaciones de tiempo real en las redes conmutadas

Las redes conmutadas está sujetan a retrasos en función de la carga, la velocidad del enlace de salida, el tamaño de los paquetes, la arquitectura del switch y el número de switches entre el servidor y el cliente. El retraso puede oscilar entre diez µs y varios ms. La mayoría de los switches son de tipo «store-and-forward» y comprueban cada paquete antes de reenviarlo. Si el switch tiene una velocidad de enlace de salida de 10 Mbit/s (puerto receptor del switch) y el tamaño del paquete es de 1.522 bytes, las tareas de «store-and-forward» provocarán un retraso máximo de 1,2 ms. Sin embargo, si la velocidad es de 100 Mbit/s, el retraso máximo será de 1,2 µs. Por eso, para poder utilizar Ethernet en aplicaciones de tiempo real es fundamental elegir la tecnología adecuada, y combinarla con sincronización horaria.

Funciones del switch

Priorización (QoS, calidad de servicio)

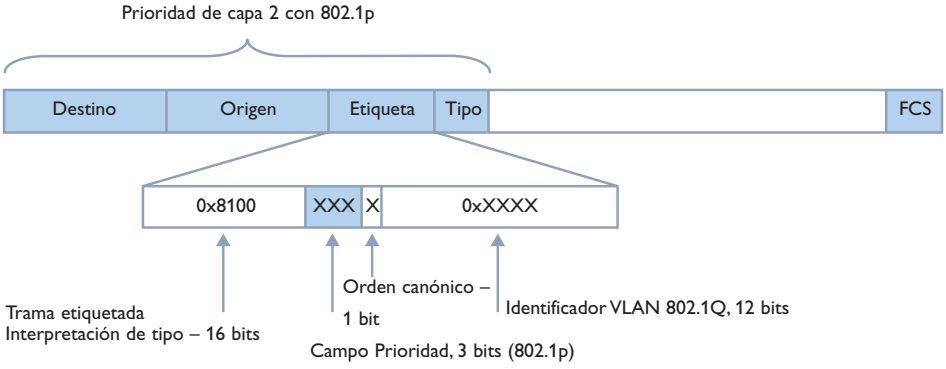
Los switches que admiten priorización tienen dos o más colas conectadas a los puertos para gestionar los datos (calidad de servicio). La priorización puede tener lugar en distintos niveles y con diferentes técnicas.

Así, el switch puede enviar un número predeterminado de paquetes desde una cola de alta prioridad antes de enviar un paquete de baja prioridad (round-robin o turno rotatorio). Otra técnica consiste en aplicar una priorización estricta, en la que todo el tráfico priorizado tiene preferencia sobre el tráfico de baja prioridad.

Prioridad de capa 2

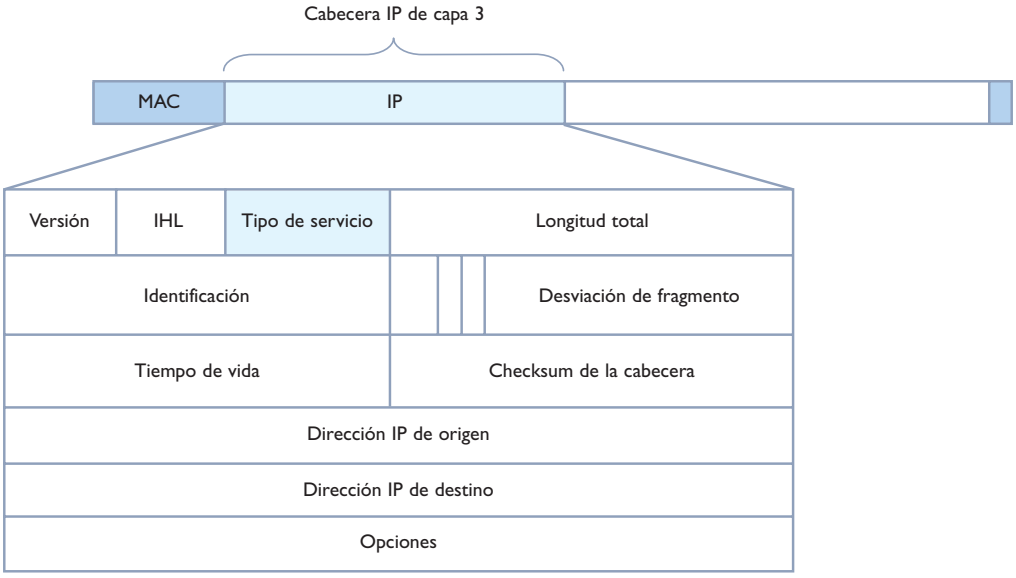
Los switches de capa 2 pueden priorizar los datos en la capa MAC a partir de los elementos siguientes:

- **Dirección MAC**: tanto la dirección de destino como la de origen se pueden utilizar para priorizar los datos. Esta opción requiere un switch de tipo gestionado, de modo que sea posible configurar la prioridad en las direcciones MAC.
- **Puerto Ethernet (capa 1)**: uno o más puertos se pueden configurar para datos de prioridad alta. Como resultado, todo el tráfico por esos puertos se gestionará como datos de alta prioridad.
- **Prioridad asignada con etiquetas**: con arreglo a la norma IEEE 802.1 p (y 802.1Q). El paquete Ethernet incluye el campo adicional Tag Control Info (TCI), es decir, un campo de información de control de etiqueta. El campo va entre los de dirección de origen y tipo, y aumenta la longitud del paquete de 1.518 bytes a 1.522 bytes. La etiqueta de información utiliza 3 bits para establecer la prioridad, lo que significa que se pueden establecer 8 niveles de prioridad.



Prioridad de capa 3

Con un switch de capa 3 se pueden priorizar los datos parcialmente en la capa MAC (capa 2), del modo descrito en el punto anterior, o en combinación con un «nivel de cabecera» IP, esto es, como un router. La prioridad se asigna a cada paquete en función del contenido del campo Type of Service (ToS) (tipo de servicio).

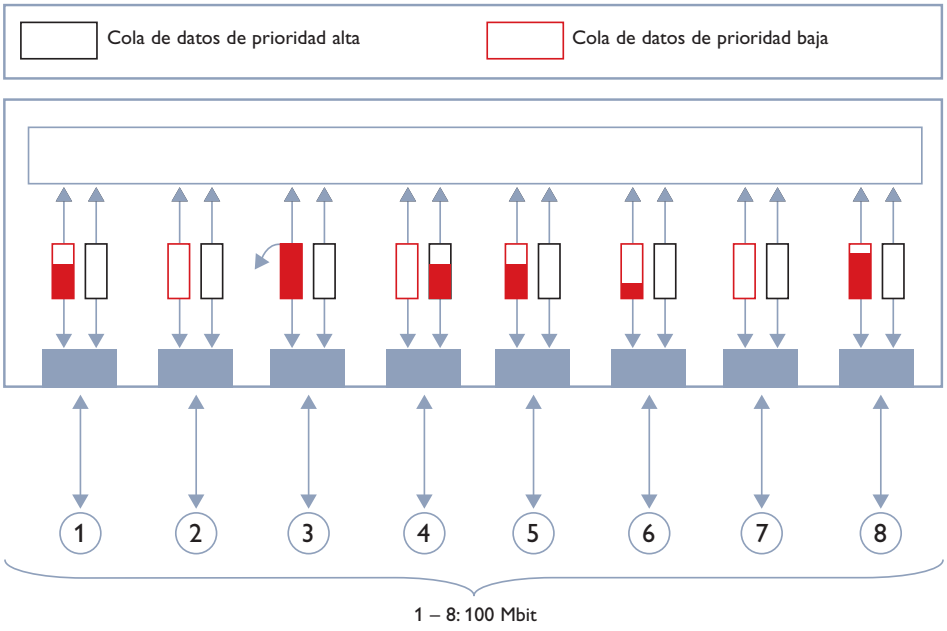


Prevención HOL (Head of Line)

Los datos entrantes y salientes se ponen en cola en el switch (gestión de colas), por lo general según un modelo FIFO (primero en entrar primero en salir). Sin embargo, cuando los datos recibidos han de ser enviados a varios puertos y uno de ellos está sobrecargado, hay que esperar hasta que el búfer sobrecargado pueda volver a recibir datos. Es lo que se conoce como prevención HOL.

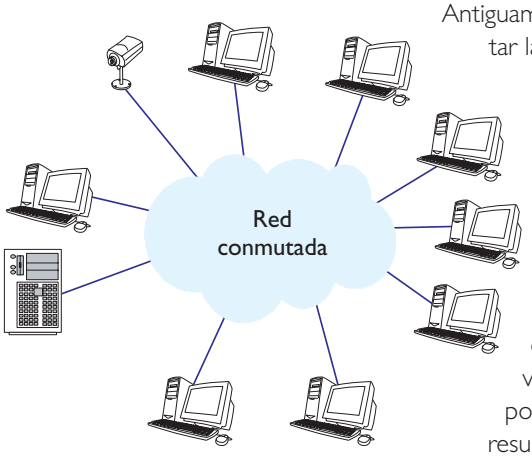
Así, si un switch tiene varias colas para datos de prioridad alta y baja, un paquete de prioridad alta se puede retrasar debido a un problema de HOL.

La prevención HOL soluciona el problema comprobando si el paquete tiene asignada prioridad y, si es así, poniéndolo en una cola aparte o descartándolo si su prioridad es baja (puerto 3 en la figura). Descartar los datos de baja prioridad no supone un gran inconveniente, dado que las aplicaciones o el protocolo TCP controlan si es preciso o no retransmitir el paquete.



VLAN

VLAN o LAN Virtual es una técnica que permite agrupar equipos en una red común. Las opciones disponibles para hacerlo son varias, bien en el nivel de puerto o bien en el nivel de dirección MAC. Además, algunos fabricantes ofrecen soluciones específicas.

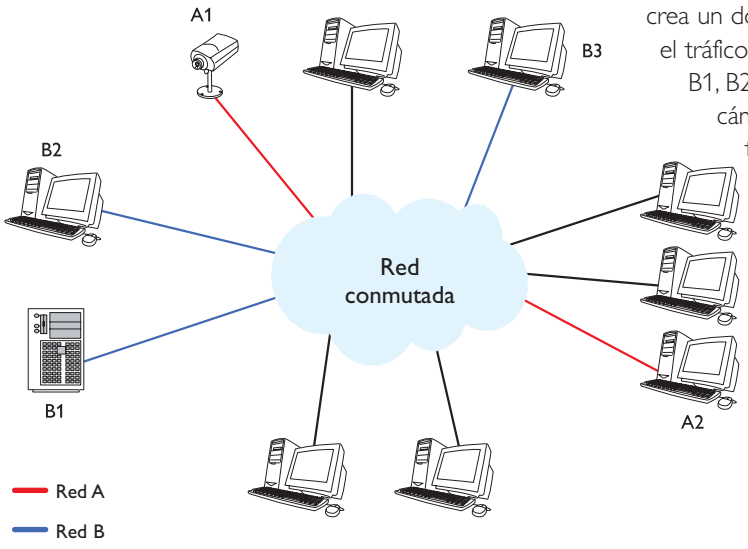


Antiguamente, las empresas y los organismos solían utilizar routers para segmentar las redes grandes, pero ahora se puede hacer lo mismo con VLAN.

Una red con equipos instalados forma un dominio de «difusión» común para todos los dispositivos conectados. Si se hace necesario ampliar la red, normalmente habrá que introducir algún tipo de segmentación, en parte debido a la velocidad pero también por las ventajas que presentan las redes segmentadas desde el punto de vista de su administración. Lo normal en estos casos es utilizar uno o más routers.

En la red, todos los equipos pertenecen al mismo dominio de difusión, pero cada conexión constituye un dominio de colisiones independiente. Debido a ello, todas las difusiones se envían a todos los dispositivos. Al ampliar la red existe el riesgo de que se produzcan más difusiones por el aumento en el número de equipos conectados y de que, como resultado, el rendimiento de la red disminuya. Además, algunos equipos pueden admitir multidifusión y transmitir datos a varios destinatarios. Si se hace necesario limitar el tráfico cosa bastante probable se puede hacer con routers o con VLAN (**V**irtual **LAN**).

El principio consiste en especificar, utilizando un switch compatible con VLAN, aquellos dispositivos que estarán en la red virtual común. La red virtual crea un dominio de difusión independiente que elimina todo el tráfico no deseado a los demás dispositivos. En el ejemplo, B1, B2 y B3 se comunican entre sí en una red virtual. La cámara de vídeo A1 envía información constantemente, pero sólo a A2. Los demás dispositivos se comunican siguiendo las reglas de una red conmutada.



IGMP/IGMP snooping

Internet **G**roup **M**anagement **P**rotocol (IGMP, protocolo de administración de grupos de Internet) es un protocolo que utilizan los servidores IP para notificar a los routers multidifusión más cercanos la pertenencia a grupos multidifusión. Los routers multidifusión envían periódicamente un «mensaje de consulta de miembros» para mantener actualizado su registro de miembros del grupo de la red local. Los servidores de la red local responden con un informe de los miembros. Los servidores sólo responden a las peticiones relativas a los grupos a los que pertenecen. Si el router no recibe el informe solicitado después de varios mensajes de consulta, da por supuesto que no queda ningún miembro en la red local y deja de reenviar a ese grupo los datagramas transmitidos a la red local por otras redes.

Generalmente la capa 2 gestiona el tráfico IP multidifusión del mismo modo que el tráfico de difusión, es decir, enviando los datos a todos los puertos. La sobrecarga resultante puede ser considerable y reducir el rendimiento de la red. Sin embargo, utilizando IGMP Snooping el switch puede filtrar el tráfico y reducir así el tráfico no deseado. La técnica consiste en que el switch «escucha» la conversación IGMP entre el servidor y el router, determina si el servidor se integra en un grupo o lo abandona y de ese modo averigua qué dispositivos pertenecen al grupo multidifusión. Actualmente hay tres niveles IGMP definidos:

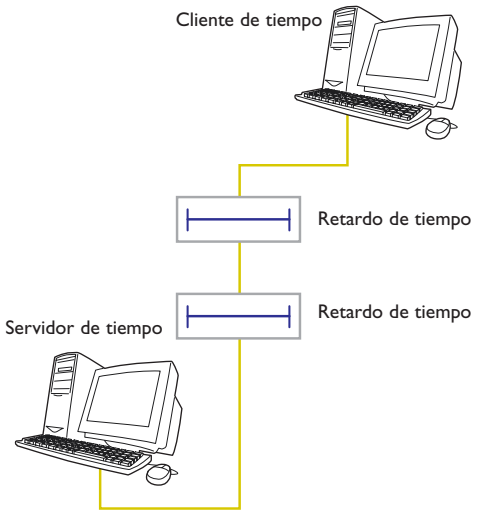
- IGMPv1 (REF 1112): versión original de IGMP, incluye el procedimiento que emplea el servidor para solicitar su integración en un grupo. Sin embargo, v1 no tiene ningún método de abandono del grupo, así que el router tiene que utilizar un temporizador para dar por finalizada la pertenencia al grupo.
- IGMPv2 (REF2236): versión que incluye el método de abandono del grupo.
- IGMPv3 (REF3376): revisión general de IGMP.

Redes con sincronización horaria

Hasta ahora, los sistemas de tiempo real distribuidos solían basarse en buses de campo. Sin embargo, las redes Ethernet conmutadas ya son una opción viable, debido, en parte, a características como el ancho de banda, la posibilidad de asignar prioridades y la especificación industrial de los equipos de red, y también, en parte, a que los precios de los equipos Ethernet han bajado mucho.

Las redes conmutadas están sujetas a retrasos variables (latencia), lo que significa que los datos transmitidos desde los nodos pueden sufrir retrasos de distinta magnitud. Una de las causas de este fenómeno es la carga que soporta la red en cada momento. La precisión de la transmisión sincronizada depende en gran medida de los siguientes factores:

1. El retraso variable de la red, que a su vez depende de la carga de la red, la velocidad, el tamaño de los paquetes y la arquitectura de los switches.
2. El protocolo empleado no reviste gran importancia en comparación con los factores anteriores, pero nosotros recomendamos SNTP y NTP, por ser protocolos normalizados con pocas limitaciones.
3. La inserción de marcas horarias en los paquetes de tiempo real entrantes y salientes, que se realiza tan cerca del hardware como es posible, esto es, en las capas inferiores del modelo OSI.



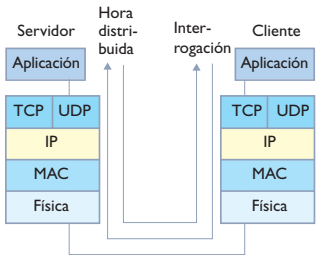
SNTP/NTP

RFC 2030 **S**imple **N**etwork **T**ime **P**rotocol (SNTP), RFC 1305 **N**etwork **T**ime **P**rotocol (NTP) y P1588 son protocolos específicos para tráfico IP sincronizado. SNTP es un subconjunto de NTP. El servidor SNTP/NTP gestiona el reloj del sistema, que puede estar basado en GPS o ser el reloj interno. La información horaria se distribuye por unidifusión o multidifusión.

1. En la actualización por unidifusión, el cliente activa el procedimiento y el servidor envía una respuesta. La referencia horaria se incluye en todas las comunicaciones entre el cliente y el servidor, con el fin de garantizar la máxima precisión.
2. En la actualización por multidifusión, el servidor envía la marca horaria a todo el grupo de clientes (grupo multidifusión) a intervalos definidos. Los clientes no pueden calcular el retraso de la red.

Inserción de marcas horarias mediante aplicaciones

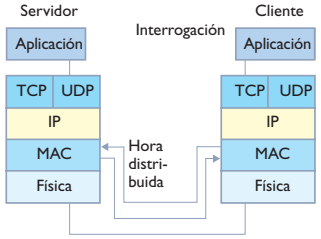
La mayoría de las aplicaciones SNTP/TCP insertan marcas horarias en la capa de aplicación, por lo que la precisión depende de las fluctuaciones/retrasos en toda la pila IP. Esta técnica ofrece una precisión típica de uno o dos milisegundos.



Inserción de marcas horarias mediante aplicaciones

Inserción de marcas horarias mediante controladores Ethernet

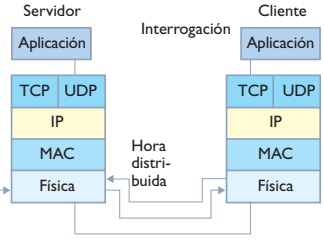
La precisión se puede mejorar significativamente insertando las marcas horarias con la rutina Ethernet de servicio de interrupción. En este caso, la inserción tiene lugar durante la transmisión de los datos entre el servidor y el cliente. Es el cliente el que genera la petición, y la precisión depende de las fluctuaciones en la gestión de interrupciones en el servidor y en el cliente. En esta aplicación, la precisión puede oscilar entre 10 µs y 100 µs.



Inserción de marcas horarias mediante controladores Ethernet

Inserción de marcas horarias en la capa física

El retraso en la pila IP se puede eliminar efectuando la inserción de marcas horarias en la capa física, es decir, por hardware. En este caso, la sincronización horaria puede ser extraordinariamente precisa (mejor de 1 µs). Sin embargo, para lograr esta precisión la conexión entre el servidor y el cliente ha de ser directa, pues los equipos intermedios aumentan el retraso. Por esta razón, el servidor de tiempo está integrado en el switch. Además, existe la posibilidad de sincronizar el switch con el reloj de referencia por GPS o mediante el oscilador interno.



Inserción de marcas horarias en la capa física

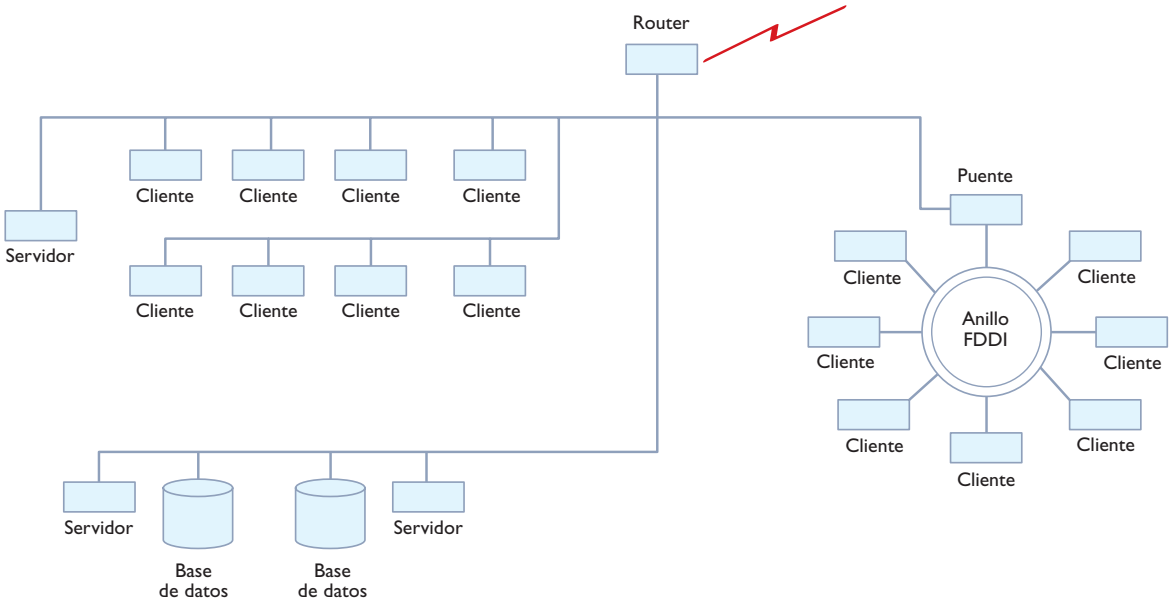
SNMP

SNMP es la abreviatura de **S**imple **N**etwork **M**anagement **P**rotocol (protocolo de gestión de red simple). SNMP permite gestionar los dispositivos de la red. Los dispositivos que se pueden supervisar se denominan agentes.

Un sistema maestro envía un mensaje de solicitud a los agentes y solicita datos, utilizando para ello una aplicación especial o Telnet.

SNMP permite:

- Supervisar tendencias.
- Supervisar eventos y analizarlos.
- Supervisar dispositivos de la red y su estado.
- Supervisar una conexión especialmente importante.
- Comprobar, con carácter preventivo, el tráfico en uno o más dispositivos de red.
- Configurar dispositivos.

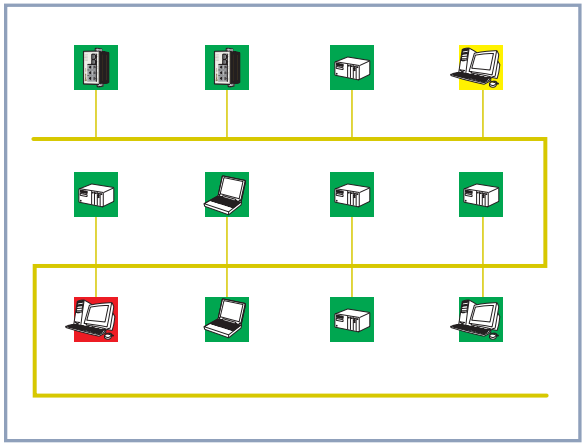


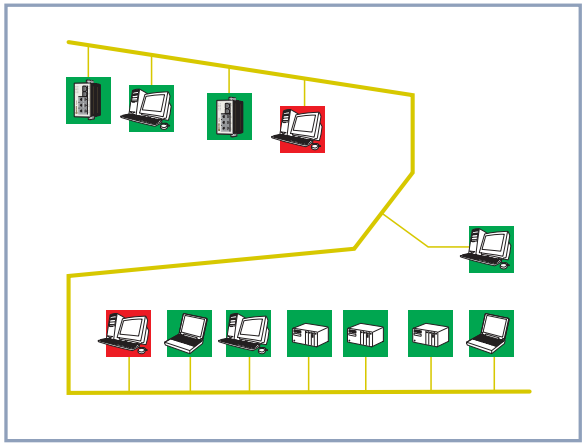
Software SNMP

El software que se emplea en la comunicación con el agente se denomina **N**etwork **M**anagement **S**olution (NMS). El intercambio de datos con los agentes es similar a la comunicación entre dispositivos maestros y esclavos, pues la comunicación con los dispositivos subyacentes se produce mediante interrogación. El administrador puede solicitar información al agente o realizar una acción en él, y éste responde a las preguntas o acciones solicitadas. Otra opción consiste en que el agente configure un «trap», que es una función controlada por evento que se activa cuando se produce una condición predeterminada, momento en el cual el agente envía los datos correspondientes al administrador.

Veamos un ejemplo:

Supongamos una red grande con equipos críticos que utilizan fuentes UPS como alimentación de respaldo. Si se produce un corte del suministro eléctrico, las unidades UPS se conectan automáticamente y los dispositivos siguen funcionando. No obstante, la condición de fallo debe enviarse de alguna manera al administrador de la red. Para ello se puede configurar un «trap» que detecte la conexión de la unidad UPS. La información se envía a un sistema **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition (SCADA, sistema de control supervisor y de adquisición de datos) en el que el administrador de la red recibe una alarma en forma de un icono que parpadea (activado por el «trap» SNMP) en la unidad UPS.





SNMP, SNMPv2 y SNMPv3

Hay tres versiones de SNMP. La versión original de SNMPv1 incluye un mecanismo de seguridad múltiple consistente en una contraseña. En la versión 1 no se puede identificar al remitente de un mensaje con certeza. Como resultado, SNMP es abierto y permite reconfigurar los dispositivos de la red, motivo por el cual muchos fabricantes de equipos no implementan todas las funciones en el estándar. Estas deficiencias se identificaron desde el principio, lo que llevó a definir una versión sustancialmente mejorada, SNMPv2, que utiliza un algoritmo de cifrado para autenticar las transmisiones entre los servidores SNMP y los agentes, y que además puede cifrar la transmisión. Sin embargo, SNMPv2, que debería haberse convertido en la evolución natural de la primera versión, no tuvo aceptación. Una de las razones fue la imposibilidad de alcanzar un acuerdo en torno a la manera de implementar la seguridad. Pese a todo, SNMPv2 fue un paso importante en el desarrollo de la siguiente versión: SNMPv3.

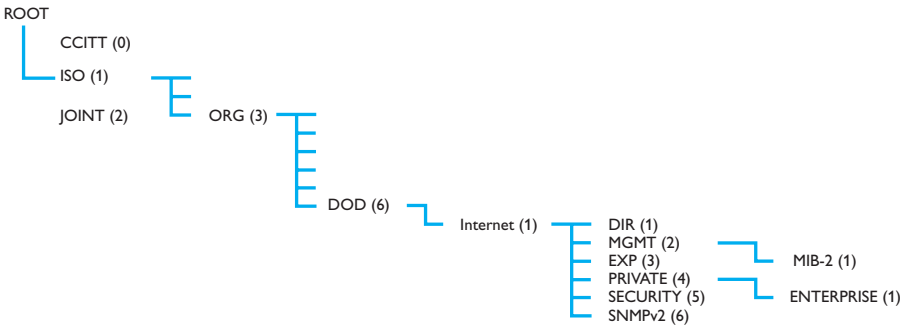
El grupo de trabajo de SNMPv3 se formó en marzo de 1997, con las tareas de examinar las propuestas de seguridad y administración recibidas y de encontrar, a partir de ellas, una solución común al problema. El trabajo debía centrarse en la medida de lo posible en completar las propuestas recibidas y no en presentar nuevas ideas. La propuesta de SNMPv3, terminada en 1998, se basó en la versión 2 y en un concepto de seguridad y de administración que se centraba en diferentes módulos que podían activarse o desactivarse según el nivel de seguridad deseado.

SNMPv3 es el estándar en uso actualmente y ofrece numerosas posibilidades de garantizar la seguridad de los dispositivos de red. Aun así, su introducción está siendo lenta; la mayoría de los dispositivos instalados aún utilizan SNMPv1.

MIB

Cada agente de la red tiene un conjunto de **M**anagement **I**nformation **B**ase (MIB, bases de información de gestión), que son objetos que el administrador puede consultar. La información puede ser estándar, como el estado del puerto, o específica de la empresa (privada), por ejemplo, la temperatura en el interior del dispositivo.

Las MIB son tablas estructuradas integradas por los diferentes objetos que puede consultar el administrador. La estructura es similar a un árbol con una raíz y directorios. En el nivel más bajo se encuentran los directorios de la MIB estándar y de las MIB privadas.



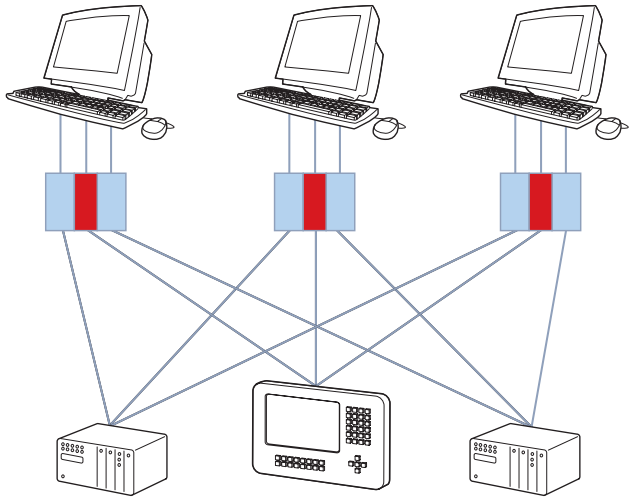
OPC

Una alternativa a SNMP es OLE for Process Control (OPC, OLE para control de procesos). Se trata de una serie de estándares específicos para el intercambio de información en centros industriales automatizados. Una de sus finalidades es mejorar la eficacia y minimizar la necesidad de utilizar controladores específicos del fabricante. En efecto, cuando se utilizan muchos controladores diferentes la implementación se complica, ya que varias aplicaciones tienen que interactuar e intercambiar información.

Las especificaciones de OPC incluyen funciones como las siguientes:

- **OPC D**ata **A**ccess (OPC DA). Acceso de datos entre aplicaciones, que permite el intercambio de información entre sistemas en tiempo real.
- **OPC H**istorical **D**ata **A**ccess (OPC HDA). Acceso al histórico de datos OPC, empleado para guardar datos de proceso antiguos y analizar tendencias.
- **OPC A**larm and **E**vents (OPC A&E). Control de alarmas y eventos.
- **OPC D**ata e**X**change (OPC DX). Intercambio de datos OPC. Define cómo debe producirse el intercambio de datos entre los diferentes servidores OPC.

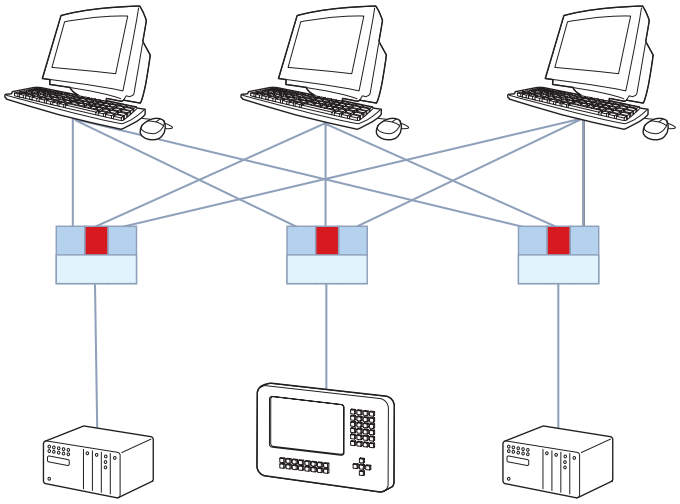
- **OPC** e**X**tensible **M**arkup **L**anguage (OPC XML). Lenguaje de etiquetado extensible para OPC. Es un lenguaje basado en HTML para el intercambio de información entre aplicaciones.



A modo de ejemplo ilustrativo de los problemas posibles, supongamos que tres aplicaciones necesitan intercambiar información entre dos PLC y un pupitre de control (HMI).

Cada fabricante tiene su aplicación específica, con sus propios controladores. Los controladores tienen que descargar datos desde los PLC y el HMI, lo que resulta en nueve puntos de integración.

OPC lo simplifica utilizando herramientas estándar. El desarrollo de OPC es el resultado de la colaboración entre los principales fabricantes de automatismos y Microsoft. Técnicamente, se utilizan COM de Microsoft (**C**omponent **O**bject **M**odel) y DCOM (**D**istributed **C**omponent **O**bject **M**odel) para las comunicaciones entre aplicaciones. En consecuencia, en nuestro ejemplo los dos PLC y el HMI tienen un punto de conexión cada uno, lo que supone una implementación más sencilla y rentable de todo el sistema.



Estas ventajas y posibilidades han llevado a los fabricantes de componentes para sistemas a incluir en sus equipos el soporte para OPC.

Ethernet por cable

Ethernet de 10 Mbit/s

Las señales que se envían por medios de 10 Mbit/s utilizan codificación Manchester, sistema que combina datos y reloj en símbolos de bit que proporcionan una transición de reloj en medio de cada bit. El cero lógico (0) se define como una señal que es mayor en la primera mitad del periodo de bit y menor en la segunda, es decir, que presenta una transición de señal negativa. El uno lógico (1) se define como una transición de señal positiva en la primera mitad del periodo de bit.

Gracias a la transición de señal, al receptor le resulta más fácil sincronizarse con la señal entrante y extraer de ella datos. El principal inconveniente es que, en el peor de los casos, la velocidad de señalización es dos veces superior a la velocidad de transmisión. Cuando no hay datos que enviar se transmite una señal de prueba de enlace.

Fast Ethernet

Los sistemas con 100Base-T como medio utilizan codificación de bloques 4B/5B, en la que los bloques de datos de 4 bits se traducen en símbolos de código de 5 bits para la transmisión por el medio. El sistema de codificación de 5 bits permite transmitir 32 símbolos de 5 bits, incluidos los 16 símbolos que transportan los datos de 4 bits y los 16 símbolos de control. Si no hay otros datos, se envía constantemente el símbolo de control IDLE. De este modo, la red está constantemente activa, enviando símbolos IDLE de 5 bits a 125 Mbit/s si no hay otra cosa que transmitir. Cada sistema de 100 Mbit/s (Fast Ethernet) utiliza diferentes medios de señalización.

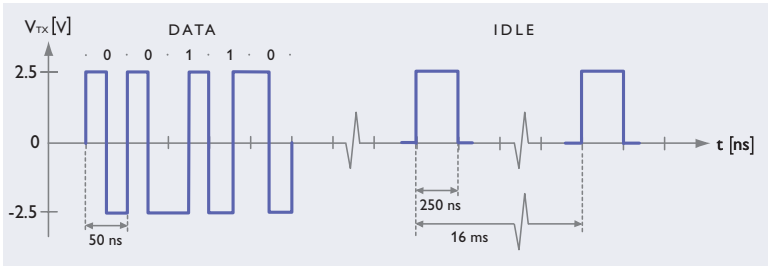
100Base-TX utiliza aleatorización y señalización multinivel de 3 niveles (MLT-3). A su paso por el cable, la señal puede tener uno de los tres niveles disponibles. Un cambio de un nivel al siguiente indica un uno lógico (1); un nivel único constante indica un cero lógico (0). Para reducir (difuminar) la emisión electromagnética, se ejecuta un proceso de aleatorización antes de modular la señal MLT-3. El aleatorizador produce una secuencia no repetitiva de bits a partir de los bits que se van a transmitir.

Los medios de fibra óptica 100Base-FX utilizan codificación NRZI. Este sistema no hace cambios en el nivel de la señal cuando se envía un cero lógico, pero invierte el nivel en los unos lógicos.

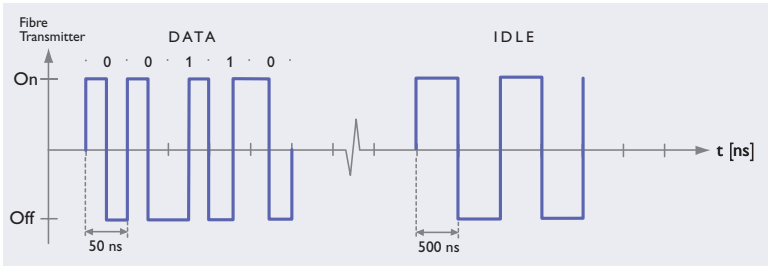
Gigabit Ethernet

El medio 1000Base-T (cobre) utiliza codificación 4D-PAM5. El sistema transmite y recibe los datos simultáneamente por cuatro pares (4D), utilizando cinco niveles de tensión (PAM5) en cada par trenzado.

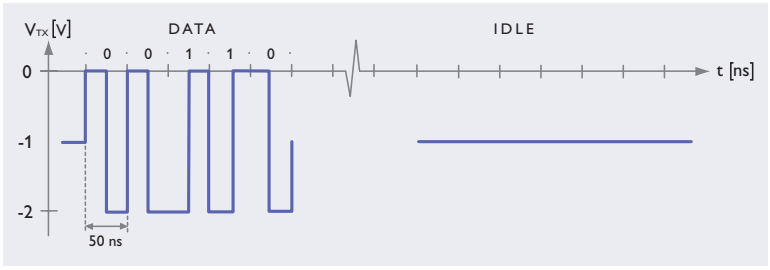
El medio 1000Base-F (fibra) utiliza codificación 8B/10B. Los datos y los símbolos de control se transmiten a una velocidad de 1.250 Mbit/s. La elevada velocidad de señalización requiere el uso de transceptores láser.



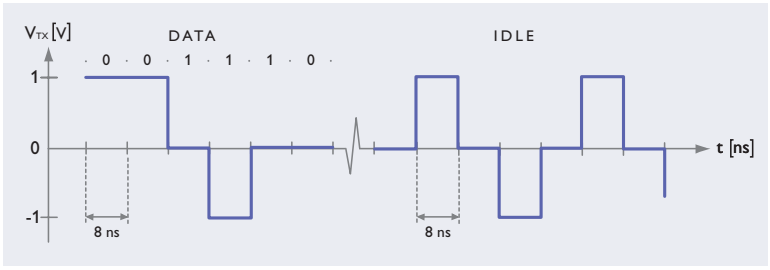
10Base-T



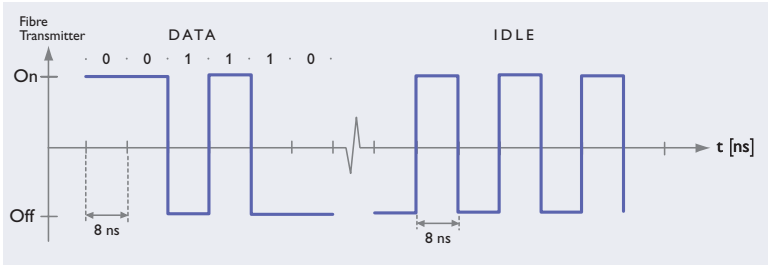
10Base-FL



10Base2



100Base-TX



100Base-FX

Glosario

10Base2	Estándar de cableado para Ethernet que utiliza cable coaxial fino como medio de transmisión. La longitud de cada segmento de la red no puede superar los 185 m. Los dispositivos se pueden conectar directamente en serie a la LAN.
10Base5	Estándar de cableado para Ethernet que utiliza cable coaxial grueso de doble pantalla como medio de transmisión. La longitud de cada segmento de la red no puede superar los 500 m. El cable va conectado a una unidad MAU (Medium Attachment Unit) para que los dispositivos se puedan comunicar a través de un puerto AUI (Attachment Unit Interface) situado en el dispositivo Ethernet.
10BaseFL	Estándar de cableado para Ethernet que utiliza cable de fibra óptica como medio de transmisión. El cable 10BaseFL ofrece una velocidad de transmisión de 10 Mbit/s.
10BaseT	Estándar de cableado para Ethernet que utiliza dos pares trenzados de hilo de cobre como medio de transmisión. La distancia máxima permitida entre los dispositivos o a un hub o un switch de red es de 100 m. Los dispositivos Ethernet se conectan con un conector de tipo RJ-45. El cable 10BaseT ofrece una velocidad de transmisión de 10 Mbit/s, mientras que la del cable 100BaseT es de 100 Mbit/s.
Aislador	Dispositivo que proporciona aislamiento galvánico entre las unidades en comunicación.
Aislamiento galvánico	Hace referencia al aislamiento eléctrico, es decir, a la inexistencia de contacto eléctrico.
ARP	El **A**ddress **R**esolution **P**rotocol (protocolo de resolución de direcciones) se utiliza para convertir direcciones IP en direcciones MAC. Dado que se trata de una herramienta TCP/IP, se utiliza para añadir o borrar información de direcciones MAC o IP.
ARQ	**A**utomatic **R**epeat re**Q**uest (petición automática de repetición).
ASCII	Sistema de codificación de datos binarios que define 128 códigos mediante diferentes combinaciones de unos y ceros. ASCII = **A**merican **S**tandard **C**ode for **I**nformation **I**nterchange.
Asíncrono	Modo de transmisión de datos en el que los caracteres se envían de uno en uno con bits de salida y parada. Aproximadamente el 90–95% de las transmisiones de datos serie son asíncronas.
Atenuación	Las señales de datos se atenúan en mayor o menor medida en función de la longitud del cable y del número de empalmes (fibra óptica).

AUI	**A**ttachment **U**nit **I**nterface Port (puerto de interfaz de la unidad de conexión). Cable Ethernet estándar con conector de tipo D de 15 patillas que se utiliza para conectar un dispositivo de red y una unidad MAU.
Auto MDI/MDI-X	Puerto Ethernet que detecta si el puerto final es un dispositivo MDI o MDI-X y configura automáticamente el puerto en consonancia.
Autodetección	Capacidad de un dispositivo Ethernet de 10/100 de interpretar la velocidad o el modo dúplex del dispositivo conectado. El dispositivo configurará automáticamente sus parámetros de manera que coincidan con la configuración requerida.
Autonegociación	La norma IEEE802.3u especifica un subnivel MAC para la identificación de la velocidad y el modo dúplex de conexión soportados por un dispositivo. El soporte de esta función es opcional.
Banda ancha	Tecnología que permite transmitir simultáneamente, por varios canales diferentes, datos, señales de audio y señales de vídeo, a frecuencias distintas.
Baudio	Es la unidad de velocidad de transmisión, en número de «paquetes» transmitidos por segundo. En la transmisión local de datos, baudio = bit/s. En telecomunicaciones, cada paquete puede contener más bits.
Bit	Un bit de datos es un dígito binario, un uno o un cero.
Bit de inicio	Constituye el comienzo de una transmisión. En la transmisión asíncrona, cada carácter va precedido de un bit de inicio.
Bit de paridad	Bit de control que se calcula matemáticamente y que el equipo de transmisión incluye en el envío. La unidad receptora comprueba la paridad y detecta cualquier error que puedan contener los datos transmitidos.
Bit/s	Unidad de medida de la transmisión de datos, en número de bits de datos por segundo.
Bits de datos	Véase el término bit.
Bits de parada	Uno o más bits de parada indican que el carácter está completo.
BOOTP	El protocolo BOOTP permite a los dispositivos de red pedir información de configuración a un servidor BOOTP.
BRI	**B**asic **R**ate **I**nterface (interfaz de velocidad básica). Servicio RDSI que proporciona acceso a dos canales B y a un canal D de 16 kbit/s.
BSC	**B**ase **S**tation **C**ontroller (controlador de estaciones base). Estación de conmutación de la red GSM que comunica las estaciones transceptoras base con la red central.

BTS
Base **T**ransceiver **S**tation (estación transceptora base). Estación base de la red GSM que establece la comunicación entre el equipo móvil y el controlador de estaciones base (BSC, Base Station Controller).

Bucle de corriente
Un bucle de corriente es un método de transmisión serie que deja pasar o interrumpe la corriente en un par.

Búfer
Memoria que puede almacenar datos durante periodos breves de tiempo, por ejemplo, mientras se espera al receptor.

Bus de campo
Estándar definido para redes de datos industriales, por ejemplo, PROFIBUS.

Bus de datos
Dispositivo formado por varios cables en paralelo y que se utiliza para la transmisión de datos dentro del equipo.

Byte
Carácter formado por dígitos binarios, por ejemplo, un carácter ASCII, que consiste en 7-8 bits de datos que se corresponden con un carácter alfanumérico.

CA
Corriente**A**lterna.

Cable coaxial
Cable con una envuelta externa apantallada y un conductor protegido para la transmisión rápida y sin interferencias de datos.

Capacidad
Aptitud para absorber una carga eléctrica.
Se mide en microfaradios = 10^{-6} F = 1 µF
nanofaradios = 10^{-9} F = 1 nF
picofaradios = 10^{-12} F = 1 pF

Carril DIN
Deutsche **I**ndustri **N**orme. Norma relativa al montaje de los equipos en compartimentos.

CAT5
Cable de par trenzado de cobre que soporta anchos de banda de hasta 100 MHz o 1000 MHz cuando se utilizan los cuatro pares. Las velocidades de transmisión normales son de 100 Mbit/s o 1.000 Mbit/s.

CAT5e
Mejora del estándar Cat5 que incluye inmunidad al ruido. Es el más común en las instalaciones nuevas.

CC
Corriente **C**ontinua.

CHAP
El **C**hallenge **H**andshake **A**uthentication **P**rotocol (protocolo de autenticación por reto) es mucho más seguro que PAP. Además de solicitar información de contraseña al iniciarse la sesión, solicita nuevas contraseñas durante el modo de reto. Si no se facilita un carácter o contraseña correcto, la conexión se interrumpe.

Checksum
Suma de comprobación. Resultado de una función matemática que controla si la transmisión de datos es correcta.

Cliente Servidor	Solución LAN en la que el procesamiento de datos y el software están repartidos entre los ordenadores personales (clientes) y un servidor.
CMV	**C**ommon **M**ode **V**oltage (tensión de modo común). Tensión longitudinal, por lo general de generación inductiva.
Codificación Manchester	Método de modulación que simplifica el bloqueo del reloj de símbolos.
Colisión	Se produce cuando dos o más dispositivos intentan transmitir datos al mismo tiempo por la misma red. Los datos que colisionan se corrompen.
Comandos Hayes	Grupo de comandos para las comunicaciones con módems telefónicos.
Conexión remota	Capacidad para conectar un equipo, a través de un medio de comunicación (GSM, RDSI, línea) a otro situado fuera del emplazamiento.
Convertidor de interfaz	Módem que convierte las señales entre dos interfaces diferentes, por ejemplo, entre RS-232 y RS-422/485.
Corrientes de tierra	Corriente que fluye por los conductores de tierra entre dos sistemas con potenciales de tierra diferentes.
CSD	**C**ircuit **S**witched **D**ata (datos de conmutación de circuitos). El método más común de transmisión de datos por la red GSM.
CSMA/CD	**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **D**etect (protocolo de acceso múltiple con detección de portadora y detección de colisiones). Método de acceso al medio Ethernet en el que todos los dispositivos luchan por acceder a la red para transmitir datos. Si un dispositivo detecta la señal de otro mientras trata de transmitir, la transmisión se interrumpe y se produce un nuevo intento transcurrido cierto tiempo.
Cuatro hilos	Cable de tipo par trenzado de 4 hilos.
Datagrama	Secuencia de datos autocontenida que transporta información suficiente para ser encaminada desde el dispositivo de origen hasta el dispositivo de destino sin que se haya producido previamente interacción alguna entre ambos. Por lo general, este tipo se conexión se conoce como comunicación no orientada a conexión.
DCE	**D**ata **C**ommunication **E**quipment (equipo terminal de datos).
DDS1	Norma europea para conexiones RDSI.
Desvanecimiento	Debilitamiento o atenuación de las señales en función de la distancia de transmisión (cable, aire, etc.).

DHCP	El **D**ynamic **H**ost **C**onfiguration **P**rotocol (protocolo dinámico de configuración de equipos) permite a los equipos solicitar (y recibir) una dirección IP de un servidor DHCP situado en la LAN. Si no se dispone de servidor DHCP, las direcciones IP deben definirse de manera estática en la configuración del dispositivo Ethernet.
Dirección IP	La dirección IP es un número de 32 bits que identifica a un dispositivo de red. Se compone de cuatro partes. En primer lugar, el identificador de una red concreta, y en segundo lugar, un identificador del dispositivo determinado dentro de la red. Dado que el número de direcciones IP formadas por un número de 32 bits es finito, actualmente se está implementando un nuevo método: el de las direcciones IPv6.
Dirección MAC	La **M**edia **A**ccess **C**ontrol Address o dirección de control de acceso al medio es un número hardware único que se asigna al dispositivo Ethernet en el momento de su fabricación. Por lo general, la dirección MAC no se puede modificar.
Divisor de línea	Divide una línea de datos sencilla en varias, por ejemplo cuando dos o más usuarios necesitan compartir el mismo equipo.
DTE	**D**ata **T**erminal **E**quipment (equipo terminal de datos).
Dúplex	Define la comunicación bidireccional. En el modo half dúplex, las partes se alternan para enviar y recibir, mientras que en el modo full dúplex lo hacen simultáneamente.
EMC	**E**lectro **M**agnetic **C**ompatibility (compatibilidad electromagnética). Hace referencia al diseño de los productos de manera que no presenten interferencias con otros equipos electrónicos.
EMI	**E**lectro **M**agnetic **I**nterference (interferencia electromagnética).
Equipo no inteligente	Dispositivo que no puede guardar datos sobre sí mismo, por ejemplo, su propia dirección en una red. Algunos ejemplos de equipos no inteligentes son los dispositivos de E/S básicos, transductores, sensores, instrumentos de medida, etc.
Esclavo	Dispositivo interrogado en un sistema de interrogación.
Ethernet	Uno de los estándares más comunes para redes de bus LAN en oficinas. En su construcción se puede utilizar tanto cable coaxial como cable especial de 4 hilos.
Etiquetado de prioridad	Capacidad de un dispositivo de red Ethernet de insertar una etiqueta en un paquete Ethernet para que tenga más prioridad que otros paquetes en la misma red.
Euro-ISDN	Solución RDSI basada en las normas europeas.
FaxMódem	Módem que puede enviar y recibir datos (texto, imágenes) en formato de fax.

FDDI	**F**ibre **D**istributed **D**ata **I**nterface. Especificación para redes de fibra óptica.
Fibra óptica	Luz láser modulada o haces láser procedentes de diodos emisores de luz conducidos a través de cristal fino o fibra de plástico, normalmente de entre 800 – 1300 nm (nanómetros). Los haces de cable de fibra pueden transmitir grandes cantidades de información.
Firewall	Router que se utiliza para ocultar las direcciones IP.
FP	P**u**erto Ethernet de fibra **ó**ptica.
FRNT	**F**ast **R**e-Configuration **N**etwork **T**opology (protocolo de reconfiguración rápida de la topología de red). Los switches Ethernet se instalan formando múltiples anillos redundantes. Para reforzar la redundancia los anillos separados se conectan por medio de enlaces de respaldo.
FTP	**F**ile **T**ransfer **P**rotocol. Este protocolo es una de las maneras más sencillas de transferir archivos por Internet. Utiliza los protocolos TCP/IP.
Full dúplex	Método de comunicación bidireccional en el que las señales pueden circular en ambas direcciones simultáneamente.
Generador de sincronismo	Frecuencia periódica que se envía desde una fuente de señales (generador de pulsos de sincronismo) y que, entre otras cosas, se utiliza para ajustar la velocidad, por ejemplo, del flujo de datos en una transmisión serie.
GPRS	**G**eneral **P**acket **R**adio **S**ervice (Servicio general de radiocomunicaciones por paquetes). Servicio GSM de transmisión de datos por conmutación de paquetes.
GPRS Attach	Interrogación del equipo GSM en relación con el permiso para conectarse a una red GPRS.
GPS	**G**lobal **P**osition **S**ystem (sistema de posicionamiento global). Sistema de navegación por satélite que utiliza 24 satélites situados en órbita alrededor del planeta. Cada satélite lleva un reloj atómico con una precisión del orden de una mil millonésima de segundo (nanosegundo).
GSM	**G**lobal**S**ystem for **M**obile communication (sistema global de comunicaciones móviles). Estándar de comunicación digital inalámbrica.
Half dúplex	Comunicación bidireccional.
Hub	Dispositivo sencillo que permite conectar segmentos de red. Cuando se recibe un paquete en un puerto, se envía a todos los puertos del hub.

IEEE802.1d	Norma en la que se define el Spanning Tree Protocol (STP, protocolo de árbol de extensión). Se trata de un método básico para ofrecer redundancia de red.
IEEE802.1p	Norma en la que se define la priorización de paquetes. Se trata de un método de priorización que utiliza la inserción de etiquetas de prioridad en los paquetes. De este modo, el paquete puede pasar por delante del tráfico de baja prioridad.
IEEE802.3	Es la norma de especificación de Ethernet.
IEEE802.3x	Norma de control de flujo Ethernet. Especifica un método de aumentar la velocidad de un switch cuando el búfer está a punto de desbordarse. Se envía un paquete que solicita al switch de origen que deje de transmitir paquetes durante cierto tiempo.
Interfaz	Estándar definido para señales, niveles eléctricos e interconexión.
Interrogación	Hace referencia al procedimiento mediante el cual el ordenador central pregunta a las unidades conectadas si tienen información que enviar.
IP	El **I**nternet **P**rotocol (protocolo de Internet) transporta los paquetes de un nodo a otro sin tener en cuenta su contenido. IP envía cada paquete en función de una dirección de destino de cuatro bytes (la dirección IP).
Itinerancia	Posibilidad de utilizar los equipos GSM en redes de distintos operadores.
LAN	Una red de área local es un grupo de ordenadores o dispositivos Ethernet que comparte una estructura de comunicaciones. El tamaño de las redes LAN oscila entre un par de dispositivos y varios cientos.
LAPM	**L**ink **A**ccess **P**rocedure for **M**odems (procedimiento de acceso al enlace para módems). Método de corrección de errores en la transmisión por módems telefónicos.
LCD	**L**iquid **C**rystal **D**isplay. Pantalla de cristal líquido.
LED	**L**ight **E**mitting **D**iode (diodo electroluminiscente). Semiconductor que emite luz cuando recibe corriente eléctrica.
Línea dedicada	Conexión de 2 ó 4 hilos arrendada a una compañía telefónica. Puede ser una conexión punto a punto o una conexión multipunto.
Línea privada	Cable de comunicaciones de propiedad privada.
M2M	**M**achine-**to**-**M**achine. Abreviatura de «comunicación máquina a máquina».
Maestro	Dispositivo principal que interroga a los dispositivos esclavos en un sistema con interrogación.

MAN	**M**etropolitan **A**rea **N**etworks. Nombre que reciben las redes que comparten varias partes, normalmente en la misma ciudad o zona.
MAU	**M**edia **A**ttachment **U**nit. La unidad de conexión al medio permite conectar un dispositivo al medio LAN. Normalmente, el medio LAN que se utiliza con este tipo de interfaz es cable coaxial. Este tipo de cable se conoce como Thicknet o Thinnet.
MDI	**M**edium **D**ependant **I**nterface. La interfaz dependiente del medio es un puerto Ethernet que permite la conexión a otros equipos de transmisión de datos (switches, hubs, etc.) sin necesidad de utilizar un cable null modem coaxial o cruzado. Estos puertos suelen denominarse puertos Uplink.
MDI-X	**M**edium **D**ependant **I**nterface – **C**rossover. La interfaz dependiente del medio con puente de cruce es un puerto Ethernet que permite conectar otros equipos terminales de datos (PC, PLC, etc.).
MIB	**M**anagement **I**nformation **B**ase. La base de información de gestión es una base de datos de objetos en la que se pueden efectuar búsquedas o interrogaciones con un sistema de gestión que utiliza SNMP.
MNP	**M**icrocom **N**etworking **P**rotocol (protocolo de redes de Microcom). Agrupa varios métodos de corrección de errores y compresión de datos para módems telefónicos.
Módem	Término derivado de las palabras **mo**dulador y **dem**odulador. El módem modula o convierte las señales digitales del ordenador en señales eléctricas para su transmisión. En el lado receptor debe haber otro módem, que se encargará de demodular o convertir las señales eléctricas nuevamente en señales digitales.
Módem de bastidor	Módem diseñado para su instalación en un bastidor de 19".
Módem de corta distancia	Modula la señal y la adapta a los diferentes cables e interfaces. El módem garantiza una transmisión segura a largas distancias. En las transmisiones locales de datos se utilizan módems de corto alcance o módems locales.
Módem de corto alcance	Modula la señal y la adapta a los diferentes cables e interfaces. El módem garantiza una transmisión segura a largas distancias. En las transmisiones locales de datos se utilizan módems de corto alcance o módems locales.
Módem local	Véase el término módem de corto alcance.
Módem PTT	Módem de transmisión de datos que utiliza la **P**ublic **T**elephone **N**etwork (red telefónica pública).

Módem telefónico	Módem de comunicación que utiliza la red telefónica.
Modulación en amplitud	Procedimiento de transmisión de datos en el que se varía la potencia de la señal, es decir, la amplitud, de la onda portadora.
Modulación en fase	Variación de la posición de las señales durante el periodo (ángulo de fase) para codificar los bits de datos. La modulación en fase se utiliza sobre todo en la transmisión digital de datos.
Modulación en frecuencia	Tecnología para transmitir datos variando la recuencia de la fonda portadora.
Monomodo	Tecnología de transmisión de señales ópticas por cables de fibra óptica. Normalmente se utiliza en la transmisión por núcleos de fibra muy finos.
MSC	**M**obile **S**witching **C**enter (centro de conmutación de servicios móviles). Centro que garantiza la interconexión entre la red GSM y la red externa, por ejemplo, RDSI y PSTN.
Multimodo	Tecnología de transmisión por fibra óptica en la que las ondas de luz se reflejan en el núcleo de fibra.
Multiplexor	Dispositivo que reduce la necesidad de cable, al permitir sustituir 2 o más líneas dedicadas por módems y una línea, estableciendo canales independientes.
Multiplexor óptico	Multiplexor para fibra óptica. Véase el término multiplexor.
Multipunto	Una de las topologías de red de datos industriales más comunes.
NMT	**N**ordic **M**obile **T**elephony (sistema nórdico telefónico móvil). Antigua red telefónica móvil analógica.
NTP	**N**etwork **T**ime **P**rotocol. Estándar de Internet que garantiza la sincronización horaria de los relojes instalados en los dispositivos Ethernet con una precisión del orden de un milisegundo. El protocolo se basa en TCP/IP.
OPC	**O**pen **P**rocess **C**ontrol. (OLE para control de procesos.) Estándar abierto que permite a los dispositivos comunicarse entre sí de forma totalmente abierta con independencia de quién haya fabricado cada uno de ellos.
Optoacoplador	Dispositivo que transmite señales luminosas, como los diodos electroluminiscentes y los fototransistores. El optoacoplador no conduce la corriente eléctrica, por lo que además proporciona aislamiento galvánico.
OSI	**O**pen **S**ystem **I**nterconnection (interconexión de sistemas abiertos). Modelo de referencia para determinar el volumen de datos que se gestionan en cada capa de comunicación durante la transmisión.

PAP	**P**assword **A**uthentication **P**rotocol. El protocolo de autenticación de contraseña envía una contraseña en texto no cifrado al servidor con fines de comparación.
Paquete	Es la unidad de datos que se transmite de un dispositivo de origen a otro de destino en Internet. Cuando un dispositivo solicita datos, la capa TCP del protocolo TCP/IP divide el archivo en paquetes. TCP/IP numera cada uno de los paquetes de tal modo que, aunque se transmitan por caminos diferentes, es posible restaurarlos correctamente en el dispositivo de destino. El tamaño de los paquetes varía entre 48 y 1.518 bytes (1.522 bytes si incluyen una etiqueta de prioridad).
Patilla	Terminal de, por ejemplo, un conector sub-D y de los circuitos diseñados para montaje a presión o soldados.
PDP Context	**I**acket **D**ata **P**rotocol. PDP Context contiene la información que define una conexión GPRS entre una MS (**M**obile **S**tation) y una red GPRS. Context define aspectos tales como el encaminamiento, la calidad de servicio QoS (**Q**uality **o**f **S**ervice), la seguridad, las tarifas, etc.
PDS	**P**remises **D**istributed **S**ystem. Hace referencia a diferentes niveles de integración de los sistemas de transmisión de datos, telecomunicaciones, calefacción, ventilación, supervisión, etc.
PLC	**P**rogrammable **L**ogic **C**ontroller (controlador lógico programable).
POTS	**P**lain **O**ld **T**elephone **S**ystem (servicio telefónico ordinario). Otra forma de referirse a la red pública telefónica conmutada (PSTN).
PPP	**P**oint to **P**oint **P**rotocol. Protocolo de comunicación que permite al PC conectarse a cualquier dispositivo Ethernet adicional a través de un enlace serie y comunicarse con él.
PRI	**P**rimary **R**ate **I**nterface (interfaz de velocidad primaria). Servicio RDSI que da acceso a un canal D de 64 kbit/s y a 30 canales B (en Europa).
PROFIBUS	Estándar de las redes de datos industriales.
Protocolo	Establece normas de transmisión de datos, la manera en que deben interrelacionarse las señales, la manera en que deben enviarse, recibirse, iniciarse y detenerse, el modo en que deben gestionarse las colas, etc.
PSI	**P**roveedor **de** **S**ervicios de **I**nternet. Empresa que proporciona un acceso a Internet.
PSTN	**P**ublic **S**witched **T**elephone **N**etwork (red pública telefónica conmutada). La red telefónica analógica común.

QoS	**Q**uality **o**f **S**ervice. Nivel de servicio y calidad definibles en los servicios de red, por ejemplo, eco, ruido, frecuencia de errores de bit, tiempos de conexión, etc.
RDSI	**R**ed **D**igital **de S**ervicios **I**ntegrados. Estándar de las redes digitales de telecomunicaciones, datos, fax, vídeo y videoconferencia.
Red	Término general con que se describen los enlaces de comunicación entre dos o más equipos.
Red en anillo	Red conectada en serie en la que todas las unidades están conectadas formando un anillo cerrado y todas las comunicaciones pasan por las diferentes unidades que lo componen.
Red en estrella	Red creada alrededor de una unidad central, desde la que salen líneas a todas las unidades conectadas.
Red telefónica	Otra forma de referirse a la red pública telefónica conmutada (PSTN).
Repetidor	Amplificador de la señal que recrea la señal y permite añadir nuevos segmentos a la red.
Resistencia	Hace referencia a la resistencia eléctrica de un cable por kilómetro.
RJ-45	Conector modular de 8 posiciones conforme con la norma ISO 8877.
RLP	**R**adio **L**ink **P**rotocol. Protocolo de corrección de errores que se utiliza en las redes GSM.
RMON	**R**emote **Mon**itoring. La supervisión remota RMON es un estándar MIB que facilita datos de diagnóstico de las redes.
Router	Un router o encaminador es un dispositivo conectado al menos a dos redes que determina el siguiente punto de red al que debe transmitirse un paquete. Normalmente, el paquete pasa por varios routers antes de llegar a su destino final. Los routers más complejos disponen de tablas de rutas que les permiten determinar el trayecto más rápido o rentable.
RS-232	Estándar americano, comunicación serie.
Segmento	Parte delimitada de una red.
Señal de estado	Indica el estado del equipo conectado, por ejemplo, encendido, preparado para recibir o preparado para enviar.
Símplex	Comunicación unidireccional.
Sincronización	Señales de confirmación y estado intercambiadas entre los equipos en contacto para comprobar el caudal de datos.

Síncrono	En este tipo de transmisión, los caracteres se envían y se reciben en una única secuencia y a velocidad constante. La velocidad se controla mediante señales de sincronismo.
Sistema binario	En este sistema, los dígitos solamente pueden uno de dos valores (uno o cero), representados por las dos posiciones que puede tener el semiconductor: con o sin corriente.
SMS	**S**hort **M**essage **S**ervice (servicio de mensajes cortos). Servicio de envío/recepción de mensajes de texto cortos por la red GSM.
Switch	Dispositivo de control manual o por software que redirige el tráfico de datos.
TCP	El **T**ransmission **C**ontrol **P**rotocol o protocolo de control de transmisión se encarga de entregar y verificar los datos transmitidos de un dispositivo a otro. El protocolo detecta los errores o datos perdidos y puede activar una retransmisión hasta que los datos se hayan recibido completos y sin errores.
TCP/IP	**T**ransmission and **C**ontrol **P**rotocol/**I**nternet **P**rotocol (protocolo de control de transmisión/protocolo de Internet). Desarrollado específicamente para Internet. Se utiliza para interconectar varias redes LAN en una red WAN que permita el intercambio de datos con independencia de su procedencia, con ayuda, entre otros, del protocolo de encaminamiento. TCP/IP, que inicialmente se basaba en UNIX, está ganando terreno como protocolo de red incluso en otros entornos.
TDM	**T**ime **D**ivision **M**ultiplexing (Multiplexación por división de tiempo). El canal se divide en ranuras de tiempo que se asignan a distintos subcanales. Véase el término multiplexor.
Terminal	Unidad sin capacidad de procesamiento propia subordinada a un ordenador central o mainframe. Un ordenador personal con capacidad de procesamiento propia también puede funcionar como terminal en algunas aplicaciones.
TFTP	**T**rivial **F**ile **T**ransfer **P**rotocol. El protocolo de transferencia de archivos trivial es un método más sencillo de transferir archivos. Utiliza UDP/IP para la transferencia.
Topología	Configuración de red.
TP	Puerto de **p**ar **t**renzado de cobre.
Trama	Una **trama** es un conjunto de datos que se transmite entre dos dispositivos Ethernet como una unidad completa con información de direccionamiento y control de protocolo. La información se transmite en serie, bit a bit.
Transferencia	Término empleado para referirse al paso de una estación transceptora base a otra durante una comunicación por la red GSM.

Transitorios	Picos de corriente elevados que provocan cambios y perturbaciones en la red.
Transmisión en paralelo	Transmisión simultánea de bits de datos por cada línea. Un carácter de 8 bits (=1 byte) requiere 8 líneas paralelas. En la comunicación de 32 bits, se transmiten simultáneamente 4 bytes por 32 líneas paralelas. La transmisión en paralelo se produce principalmente en el propio equipo de datos y a distancias muy cortas.
Transmisión serie	Significa que los caracteres se envían de uno en uno por una sola línea, al contrario de lo que ocurre en la transmisión en paralelo.
UDP	El **U**ser **D**atagram **P**rotocol o protocolo de datagramas de usuario se encarga de transmitir los datos de un dispositivo a otro. Normalmente utiliza IP en la transmisión, pero al contrario de TCP, no permite dividir el mensaje en paquetes que puedan restaurarse correctamente una vez llegados a su destino. Por consiguiente, la aplicación que utilice UDP debe ser capaz de detectar que el mensaje o los datos se han recibido correctamente. Con todo, UDP tiene la ventaja de que transmite los datos a mayor velocidad y con menos sobrecarga que TCP. UDP es ideal en las aplicaciones que requieren la transmisión de volúmenes reducidos de datos a gran velocidad.
Unix	Sistema multiusuario para mainframes y miniordenadores que puede gestionar muchos procesos simultáneamente.
V.24	Estándar americano, comunicación serie.
WAN	Una **W**ide **A**rea **N**etwork, o red de área extendida es una red de comunicaciones geográficamente dispersa.
Watchdog	Circuito de comprobación que supervisa y reinicia automáticamente las funciones del módem.
VN4	Norma francesa para conexiones RSDI.