

# Indice

<b>0. Debate Inicial</b>	<b>5</b>
0.1 Definiciones.-	5
0.2 Sistema Informático.-	5
0.3 Información Digital	5
0.4 Sistemas de numeración	5
0.4.2 Sistemas de numeración binario	6
0.4.3 Sistemas de numeración octal	6
0.4.4 Sistemas de numeración hexadecimal	6
0.5 Conversión de base n a decimal	6
0.6 Conversión de decimal a base n	6
0.7 Representación en punto flotante	6
0.8 Conversión de base n a base n	6
<b>TEMA 1.- La vida en un mundo centrado en la red</b>	<b>7</b>
1. Introducción	7
La necesidad de las redes	7
2. Redes de área local LAN	8
2.1 Ventajas de las LAN	9
3. Redes de área extensa WAN	9
4. LAN vs WAN	10
5. Otras redes MAN y WLAN	10
5.1. Internet: una red de redes	11
5.2 Internetwork	11
5.3 Intranet	11
6. Elementos de una red	11
7. La topología de la red	12
7.1 Topologías más comunes	12
8. Protocolo de red	13
9. Organismos de normalización	13
<b>Tema 2 comunicación a través de la red</b>	<b>15</b>
1. Introducción	15
2. Comunicación de mensajes	15
3. Dispositivos finales	16
4. Dispositivos intermediarios	16
5. El protocolo de comunicaciones	17
6. El concepto de capa o nivel	17
7. El interface entre capas	18

<b>8. La arquitectura de una red</b>	<b>18</b>
8.1 Esquema de la estructura del modelo de capas de una arquitectura de red	18
<b>9. El modelo de referencia OSI</b>	<b>19</b>
9.1 Capas del modelo OSI	19
9.1.1 Nivel o capa física	19
9.1.2 Nivel o capa de enlace	20
9.1.3 Nivel de red	20
9.1.4 Nivel de transporte	20
9.1.5 Nivel de sesión	21
9.1.6 Nivel de presentación	21
9.1.7 Nivel de aplicación	21
9.2 Comunicación entre dos estaciones	22
9.3 Problema de OSI	22
9.4 Transmisión de datos en el modelo OSI	22
9.5 Tipos de servicios definidos en OSI	22
<b>10. Arquitectura TCP/IP</b>	<b>23</b>
10.1 Capas TCP/IP	23
<b>11. Unidad de datos del protocolo y encapsulación</b>	<b>24</b>
<b>12. Direccionamiento en la red</b>	<b>25</b>
13. Proceso de envío y recepción	25
14. Envío de datos a la aplicación correcta	25
<b>TEMA3.- Sistema de cableado estructurado</b>	<b>25</b>
<b>1. La capa física</b>	<b>25</b>
<b>2. Capa física. Funcionamiento</b>	<b>26</b>
<b>3. Capa física. Estándares</b>	<b>26</b>
<b>4. Métodos de señalización</b>	<b>27</b>
4.1 Características de las señales	27
<b>5. Capacidad para transportar datos</b>	<b>28</b>
<b>6. Medios de transmisión</b>	<b>29</b>
6.1 Medios de cobre	29
6.1.1 Par sin trenzar (paralelo)	29
6.1.1 Par sin trenzar (paralelo) II	29
6.1.2. Par trenzado	29
6.1.3 Cable coaxial	33
6.2 Fibra óptica	33
6.2.1 Tipos de fibra óptica	33
6.2.2 Ventajas e inconvenientes	34
6.2.4 Fibra óptica vs Cables de cobre	34
6.3 Medios inalámbricos	35

<u>7. Cableado estructurado</u>	<u>36</u>
7.1 Elementos del cableado estructurado	36
7.2 Longitudes máximas de cable de cobre	37
7.3 Dispositivos de conexión de cables	37
7.5 Herramientas utilizadas en la conectorización	38
7.6 Etiquetado de cables	39
7.7 Elementos de la instalación	39
7.8 Certificación de la instalación	40
7.9 El proyecto de instalación	41
<b>TEMA 4 Nivel de enlace</b>	<b>42</b>
<u>1. Introducción</u>	<u>42</u>
<u>2. La capa de enlace</u>	<u>42</u>
<u>3. PDU de la capa de enlace</u>	<u>43</u>
3.1 Función del encabezado	43
3.2 Formateo de datos para la transmisión	44
3.3 Direccionamiento: hacia donde se dirige la trama	44
3.4 Función de trailer	44
<u>4. Conexión de servicios de capa superior a los medios</u>	<u>45</u>
<u>5. Subcapas de enlace de datos</u>	<u>46</u>
<u>6. Estándares</u>	<u>46</u>
<u>7. Control de acceso al medio</u>	<u>47</u>
7.1 Control de acceso al medio para medios compartidos	47
<u>8. Control de acceso al medio para medios no compartidos</u>	<u>49</u>
8.1 Full Duplex y Half Duplex	49
<u>9. Comparación entre la topología lógica y la topología física</u>	<u>50</u>
9.1 Topología punto a punto	50
9.2 Topología multiacceso	51
9.3 Topología en anillo	51
<u>10. Protocolos de la capa de enlace de datos</u>	<u>52</u>
10.1 Protocolo Ethernet para LAN	52
10.1 Protocolo Ethernet para LAN (II)	52
10.2 Protocolo punto a punto para WAN	52
10.3 Protocolo inalámbrico para LAN	53
<u>11. Ethernet</u>	<u>53</u>
11.1 Control del enlace lógico	53
11.2 MAC: envío de datos a los medios	54
11.3 Primeros medios Ethernet	55
11.4 La trama Ethernet	55
<u>12. Ethernet unicast, multicast y broadcast</u>	<u>58</u>

12. Ethernet unicast, multicast y broadcast	58
13. Hub	58
13.1 Ethernet antigua	59
14. Switch	59
14.1 Ancho de banda dedicado	60
14.2 Funcionamiento del switch	60
14.2.1 Aprendizaje	60
14.2.2 Actualización	60
14.2.3 Inundación	61
14.2.4 Reenvío selectivo	61
14.2.5 Filtrado	61
15. El protocolo ARP	61
15.1 Resolución de direcciones IPv4 a direcciones MAC	62
15.2 Mantenimiento de una tabla ARP	62
15.2 Mantenimiento de una tabla ARP	62
15.3 El proceso de ARP: destinos fuera de la red local	62
15.4 Eliminación de mapeos de direcciones	63

# 0. Debate Inicial

## 0.1 Definiciones.-

La informática es una ciencia que estudia métodos, informática procesos y técnicas, con el fin de almacenar, procesar y transmitir información y datos en formato digital. Una computadora es una máquina electrónica que recibe y procesa datos para convertirlos en información útil.

## 0.2 Sistema Informático.-

Un sistema informático es el “conjunto de dispositivos que estarán física y lógicamente conectados entre sí (local y/o remotamente) que interactuarán con el usuario para el proceso y tratamiento de información”.

### Elementos de un SI:

- Hardware (sistema físico)
- Software (sistema lógico): Sistema Operativo + Aplicaciones
- Usuarios

## 0.3 Información Digital

Un sistema informático maneja información de todo tipo (números, texto, imágenes, audio, vídeo, etc) utilizando como soporte dispositivos electrónicos, más concretamente electrónica digital que maneja la información binaria

## 0.4 Sistemas de numeración

Un sistema de numeración es la representación de números en las que cada uno es representado de manera única. También puede definirse como la representación de cantidades numéricas como potencias sucesivas de una determinada base. El más usual es el sistema de numeración decimal.

### numeración decimal

Es el sistema de numeración usado en la vida cotidiana. Su base de numeración es 10, esto quiere decir que dispone de 10 signos para representar los números (0,1,2,3,4,5,6,7,8 y 9).

**Funcionamiento del sistema decimal: La primera posición es 10 elevado a la potencia 0, la segunda posición es 10 elevado a la potencia 1, la tercera posición es 10 elevado a la potencia 2...**

El teorema fundamental de la numeración establece que el valor en el sistema decimal de una cantidad expresada en otro sistema de numeración viene dado por la fórmula:  $N = \sum d(i).base(i)$  Ejemplo: Si queremos obtener el valor decimal del número 352 expresado en

base 6 según el teorema fundamental de la numeración:  $N = 2 * 6^0 + 5 * 6^1 + 3 * 6^2 = 139$

#### **0.4.2 Sistemas de numeración binario**

Los ordenadores utilizan una arquitectura basada en este sistema de numeración.

Su base de numeración es 2, lo que significa que dispone de dos números, el 0 y el 1, los cuales reciben el nombre de bit.

El sistema binario es el alma del ordenador y es la forma en la que están representados internamente los datos.

Un byte es una secuencia de 8 bits

#### **0.4.3 Sistemas de numeración octal**

Este sistema consta de 8 símbolos, desde el 0 hasta el 7. Octal Binario

Cada dígito en octal se puede representar como una combinación de 3 dígitos binarios.

#### **0.4.4 Sistemas de numeración hexadecimal**

Para poder representar cantidades en el sistema de numeración hexadecimal necesitamos 16 símbolos: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Cada dígito en hexadecimal puede representar con 4 dígitos binarios

### **0.5 Conversión de base n a decimal**

Coger el número y multiplicar de derecha a izquierda cada dígito por la base de numeración del número elevada al valor de su posición, comenzando por la posición cero.

### **0.6 Conversión de decimal a base n**

Conversión mediante división repetitiva.

Se coge el número decimal original, y se va dividiendo sucesivamente por la base a la que se quiere pasar el número. Una vez finalizadas las divisiones el número se formará cogiendo como primer dígito el último cociente obtenido y concatenándolo con los restos en orden inverso a su obtención.

#### **0.7 Representación en punto flotante**

Para representar un número en punto flotante (un número que contiene un entero y una fracción), el número se divide en dos partes: el entero y la fracción.

Convertir la parte entera a binario.

Convertir la fracción a binario.

Poner un punto decimal entre las dos partes.

#### **0.8 Conversión de base n a base n**

En este caso, en primer lugar se pasa el número en la base origen a base 10 y después, el resultado obtenido se pasa a la base destino.

Esta es la única forma siempre y cuando las bases no tenga ninguna relación entre sí.

En el caso de las bases 8 y 16 que son múltiplos de 2, este paso intermedio no hace falta, ya que la conversión se haría mediante su correspondencia en dígitos binarios.

# TEMA 1.- La vida en un mundo centrado en la red

## 1. Introducción

Los ordenadores son máquinas especializadas en procesar información. Sin embargo, no siempre la información se produce o se almacena en el lugar donde se procesa. Por lo tanto, existe la necesidad de transportar los datos desde un lugar de origen o almacenamiento hasta el de su proceso, originando una comunicación.

**En todo proceso de comunicación se pueden distinguir una serie de elementos básicos: El emisor y el receptor son los elementos finales.** Los traductores convierten señales acústicas en señales eléctricas susceptibles de ser enviadas a través de líneas telefónicas, que constituyen el canal de transmisión.

El **emisor** es el elemento terminal de la comunicación que se encarga de proporcionar la información. El **receptor** es el elemento terminal de la comunicación que recibe la información procedente de un emisor.

Puede darse el caso, de que emisor y receptor no estén perfectamente definidos ya que actúan indistintamente como emisor y como receptor. Ejemplo: una comunicación telefónica.

El **canal** es el elemento que se encarga del transporte de la señal sobre la que viaja la información que pretenden intercambiar emisor y receptor.

Antes de comenzar a comunicarnos, establecemos reglas o acuerdos que rigen la conversación. Estas reglas o protocolos deben respetarse para que el mensaje se envíe y comprenda correctamente.

**Algunos de los protocolos que rigen con éxito las comunicaciones humanas son: emisor y receptor identificados, método de comunicación consensuado (cara a cara, teléfono, carta, whatsapp), idioma y gramática comunes, velocidad y puntualidad en la entrega, y requisitos de confirmación o acuse de recibo.**

Las reglas de comunicación pueden variar según el contexto. Si un mensaje transmite un concepto importante, se necesita una confirmación de que se recibió y comprendió correctamente. Los mensajes menos importantes pueden no requerir acuse de recibo por parte del receptor. Las técnicas utilizadas en las comunicaciones de red comparten estos fundamentos. Al establecer las redes de datos, es necesario ser mucho más explícito sobre la forma en que se realizan y juzgan con éxito las comunicaciones.

### **La necesidad de las redes**

La información no se produce necesariamente en el mismo punto geográfico en que se procesa, lo que genera una necesidad de transporte de los datos de un lugar a otro. Se hace indispensable diseñar entidades de comunicaciones flexibles en donde sea posible la compartición de los recursos de comunicaciones.

Estas entidades de comunicación son las redes de comunicaciones, que son las encargadas de mover los datos de unos lugares a otros.

**Llamamos velocidad de transferencia de datos de una red a la cantidad de datos que es capaz de mover en cada unidad de tiempo.**

Las unidades de información comúnmente utilizadas en informática son:

Byte 8 bits

KByte 1024 bytes

MByte 1024 Kbytes

GByte 1024 Mbytes

Todas estas unidades se pueden expresar referidas a los bits en lugar de a los bytes.

Por tanto, unidades de velocidad de transferencia típicas serán el Kbps (kilobit por segundo), el Mbps (megabit por segundo), etc

## 2. Redes de área local LAN

**Una red de área local (LAN, Local Area Network)** es un conjunto de elementos físicos y lógicos que proporcionan interconexión entre dispositivos en un área **privada** y **restringida**.

La red de área local tiene las siguiente características:

- Una restricción geográfica: el ámbito de una oficina, de la planta de un edificio, un edificio entero e incluso, un campus universitario.
- La velocidad de transmisión debe ser relativamente elevada.
- La red de área local debe ser privada, toda la red pertenece a la misma organización.
- Fiabilidad en las transmisiones. La tasa de error en una red de área local debe ser muy baja. Son, por tanto, redes muy seguras.
- La red de área local debe proporcionar los servicios de comunicaciones más comunes: la **compartición** de recursos entre los distintos usuarios de la red. La principal función de una red consiste en permitir que los recursos de los ordenadores de la red se compartan entre todos los usuarios autorizados.

**Hay dos maneras de conexión de ordenadores personales en una red dependiendo de la ubicación de los recursos:**

**.- Redes entre iguales**

**.- Redes cliente/servidor**

La forma básica consiste en hacer que todos los ordenadores pongan a disposición de los demás los recursos de que disponen (principalmente discos e impresoras). Así, todos los ordenadores tienen las mismas funciones, no hay privilegios.



Tecnológicamente, este modo de organización es muy simple, pero se hace muy difícil el control de los recursos, puesto que los accesos cruzados son posibles en cualquier dirección. A este tipo de redes se les llama redes entre **iguales ó peer to peer (P2P)**.

Otra forma consiste en privilegiar al menos a uno de los ordenadores añadiéndoles capacidades en forma de servicios, por ello, a estos ordenadores, se les llama servidores o servers.

El resto de los pcs de la red solicitarán servicios a estos servidores que estarán altamente especializados en la función para la que fueron diseñados.

Esta organización es más fácil de organizar puesto que la administración de los servicios de la red está centralizada.

Los servidores llevan incorporado un sistema de cuentas y de contraseñas de entrada que restringe los accesos a usuarios no autorizados.

A este tipo de organización se le llama **cliente-servidor**.

## 2.1 Ventajas de las LAN

**Razones económicas:** compartir periféricos evita la necesidad de que cada nodo de la red tenga todos los recursos localmente. Cuando alguien necesita imprimir puede hacerlo por su impresora loca, si la tiene, o por una impresora corporativa, compartida por toda la oficina.

**Accesibilidad a los datos:** es necesario un sistema en el que los distintos usuarios de la red intercambien su información con el fin de facilitar una cooperación entre ellos.

**Evitar redundancias inútiles de la información:** en sistemas aislados, cuando distintos usuarios utilizan la misma información, cada uno debe poseer una copia de los datos que utilizará. Al disponer en el sistema múltiple copias no sincronizadas, se pueden producir desfases en la información original que impide precisar cuál de todas las copias debe tomarse como correcta. Con la utilización de LANs se evita que haya información redundante y contradictoria ya que todos los usuarios de la red trabajan con la misma copia de información.

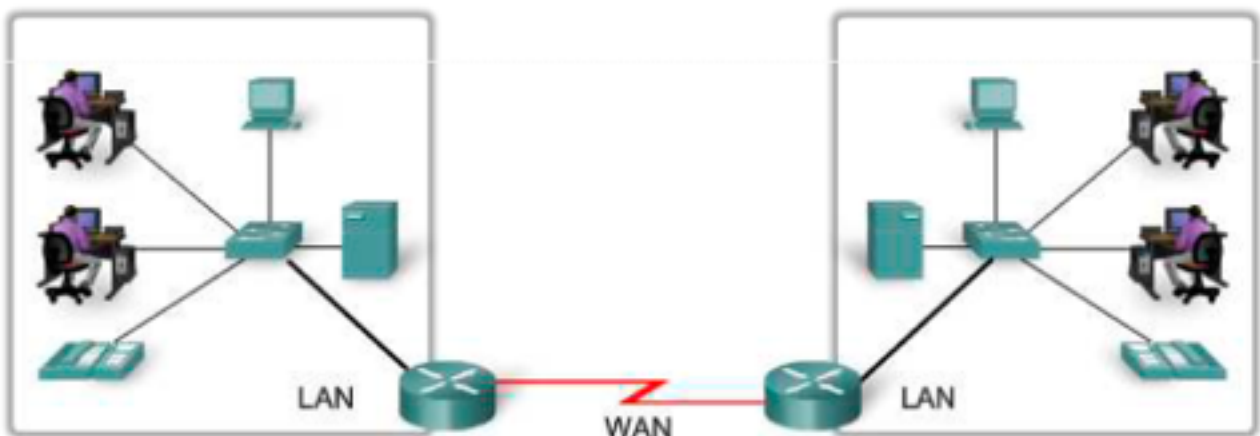
## 3. Redes de área extensa WAN

Una **red de área extensa (WAN, Wide Area Network)** es una red que intercomunica equipos en un área geográfica muy amplia por lo que son redes que conectan las LAN en ubicaciones separadas geográficamente. Las transmisiones en una WAN se realizan a **través de líneas públicas**.

Su capacidad de transmisión suele ser menor que las utilizadas en las LAN. Las tasas de error en las transmisiones en las WAN son mayores (unas 1000 veces superior) que su equivalente a las redes de área local.

## 4. LAN vs WAN

Las LAN separadas por una distancia geográfica están conectadas por una red que se conoce como Red de área extensa (WAN).



## 5. Otras redes MAN y WLAN

**Redes metropolitanas (MAN):** es una red de distribución de datos para un área geográfica en el entorno de una ciudad. Son apropiadas, por ejemplo, para la distribución de TV por cable en el ámbito de una población sobre la que se extiende geográficamente la red. Su tasa de error es mayor que las LAN y menor que las WAN.

**Redes inalámbricas:** redes sin cables. Por ejemplo: Bluetooth e infrarrojos para bajas tasas de transferencia, WiFi para redes de área local y WiMAX para redes metropolitanas. Todas estas tecnologías se agrupan bajo el nombre de WLAN (Wireless Local Area Network). Sus inconvenientes son:

- Al ser aéreo el medio de transmisión y por tanto abierto a cualquier dispositivo que se encuentre en las cercanías, las redes inalámbricas exponen una mayor superficie de ataque, lo que brinda más posibilidades a los crackers.
- Como el canal de transmisión es compartido por todas las estaciones, el ancho de banda del canal también lo será, lo que produce situaciones de congestión.

## 5.1. Internet: una red de redes

Aunque existen beneficios por el uso de una LAN o WAN, la mayoría de los usuarios necesitan comunicarse con un recurso u otra red, fuera de la organización local.

Los ejemplos de este tipo de comunicación incluyen:

- enviar un correo electrónico a un amigo en otro país,
- acceder a noticias o productos de un sitioWeb,
- obtener un archivo de la computadora de un vecino,
- mensajería instantánea con un pariente de otra ciudad, y
- seguimiento de la actividad de un equipo deportivo favorito a través del teléfono celular.

## 5.2 Internetwork

Una malla global de redes interconectadas (internetworks) cubre estas necesidades de comunicación humanas. Algunas de estas redes interconectadas pertenecen a grandes organizaciones públicas o privadas, como agencias gubernamentales o empresas industriales, y están reservadas para su uso exclusivo.

La internetwork más conocida, ampliamente utilizada y a la que accede el público en general es **Internet**.

Internet se crea por la interconexión de redes que pertenecen a los **Proveedores de servicios de Internet (ISP)**.

Estas redes ISP se conectan entre sí para proporcionar acceso a millones de usuarios en todo el mundo.

## 5.3 Intranet

El término **intranet** se utiliza generalmente para referirse a una conexión privada de algunas LAN yWAN que pertenecen a una organización y que está diseñada para que puedan acceder solamente los miembros y empleados de la organización u otros que tengan autorización.

## 6. Elementos de una red

Todas las redes tienen cuatro elementos básicos en común

1. Reglas y acuerdos para regular cómo se envían, redireccionan, reciben e interpretan los mensajes
2. Medios que puede transportar los mensajes de un dispositivo a otro
3. Mensajes que viajan de un dispositivo a otro
4. Dispositivos de la red que cambian mensajes entre sí

Utilizamos la palabra mensajes como un término que abarca las páginas Web, los e-mails, los mensajes instantáneos, las llamadas telefónicas y otras formas de comunicación permitidas por Internet.

Entre los principales dispositivos que se utilizan para administrar y direccionar los mensajes se encuentran:

**Switch:** el dispositivo más utilizado para interconectar redes de área local.

**Firewall:** proporciona seguridad a las redes.

**Router:** ayuda a direccionar mensajes mientras viajan a través de una red.

**Router inalámbrico:** un tipo específico de router que generalmente se encuentra en redes domésticas.

Para que funcione una red, los dispositivos deben estar interconectados. Las conexiones de red pueden ser con cables o inalámbricas.

En las conexiones con cables, el medio puede ser cobre, que transmite señales eléctricas, o fibra óptica, que transmite señales de luz. En las conexiones inalámbricas, el medio es la atmósfera de la tierra o espacio y las señales son microondas.

## 7. La topología de la red

**La topología de red** es la disposición física en la que se conecta una red de ordenadores, es decir, la forma en la que se interconectan los diferentes nodos o usuarios de ella.

### 7.1 Topologías más comunes

**Topología en bus:** utiliza un único cable para conectar los equipos, por lo que es la que menos cableado requiere y la más sencilla de instalar. La ruptura del bus impide la comunicación entre cualesquiera dos nodos de la red, lo que hace que esta topología sea muy sensible a la ruptura del cable. Si falla algún enlace, todos los nodos quedan aislados. Utilizada cuando el número de nodos no es excesivo.

**Topología en anillo:** todos los nodos están conectados a una única vía con sus dos extremos unidos. Al igual que ocurre con la topología en bus, si falla algún enlace, la red deja de funcionar completamente.

**Topología en estrella:** los equipos se conectarán a un nodo central con funciones de distribución, conmutación y control. Si el nodo central falla, queda inutilizada toda la red. Si falla un nodo de los extremos, sólo éste quedará aislado.

Su principal inconveniente es que todos los segmentos deben terminar en él, produciendo una importante madeja de cables. Además, el gasto de cableado es mayor.

**Topología en malla:** es una interconexión total de todos los nodos, con la ventaja de que si una ruta falla, se puede seleccionar otra alternativa. Como inconveniente destaca que es más difícil de construir y que hace falta más cable.

**Topología en árbol:** es una forma de conectar nodos como una estructura jerarquizada. Es la menos utilizada ya que el fallo de un nodo o enlace deja a conjuntos de nodos incomunicados entre sí. Sin embargo, se utiliza ampliamente en redes de telefonía donde los enlaces intermedios son centralitas locales y regionales.

**Topología irregular:** cada nodo debe estar conectado, como mínimo, por un enlace, pero no existen más restricciones. Es la más utilizada en redes que ocupan zonas geográficas amplias. Esta topología permite la búsqueda de rutas alternativas cuando falla algunos de los enlaces.

## 8. Protocolo de red

Toda comunicación, ya sea cara a cara o por una red, está regida por reglas predeterminadas denominadas protocolos. Los protocolos son las reglas que utilizan los dispositivos de red para comunicarse entre sí.

Actualmente el estándar de la industria en redes es un conjunto de protocolos denominado TCP/IP (Protocolo de control de transmisión/Protocolo de Internet).

TCP/IP se utiliza en redes comerciales y domésticas, siendo también el protocolo primario de Internet.

Son los protocolos TCP/IP los que especifican los mecanismos de formateo, de direccionamiento y de enrutamiento que garantizan que nuestros mensajes sean entregados a los destinatarios correctos.

## 9. Organismos de normalización

Inicialmente, las empresas construían las redes comprando los elementos de la red a distintos fabricantes. Cuando necesitaron comunicar esas redes, surgieron dos problemas:

- Los sistemas de transmisión no eran compatibles.
- Había que deshacerse de todo lo instalado y montar redes nuevas o había que desarrollar equipos adaptadores de redes = Coste muy elevado

Se hizo necesario definir un conjunto común de normas que permitiera coordinar a todos los fabricantes.

Estas normas posibilitan la comunicación entre diferentes equipos y permiten que éstos tengan un menor coste y una mayor aceptación.

Las normas se dividen en dos categorías:

**Estándares de facto (de hecho):** a este grupo pertenecen los estándares que simplemente aparecieron y se impusieron en el mercado por su extensa utilización. Ejemplos: el PC de IBM porque la mayoría de los fabricantes copiaron sus equipos con mucha exactitud ó el sistema operativo Unix que ha sido copiado por otros fabricantes como Minix, Linux, etc.

**Estándares de jure (por ley):** se trata de estándares formales y legales acordados por algún organismo de estandarización autorizado.

Existen varias organizaciones internacionales dedicadas a tareas de normalización y estandarización:

**ITU (International Telecom Union):** organización de las Naciones Unidas con sede en Ginebra y constituida por las autoridades de Correos, Telégrafos y Teléfonos de los países miembros. Se encarga de realizar recomendaciones técnicas sobre teléfono, telégrafo e interfaces de comunicación de datos.

**ISO (International Standards Organization):** organización de carácter voluntario que agrupa a 89 países. Uno de sus comités se ocupa de los sistemas de información, que ha desarrollado el modelo de referencia OSI y protocolos para varios niveles de ese modelo. ISO también ha desarrollado estándares en otros campos como:

- ISO 216: para medidas de papel como A4
- ISO 9000: sistemas de gestión de calidad
- ISO 3166: códigos de países

**ANSI (American National Standards Institute):** asociación con fines no lucrativos, formada por fabricantes, usuarios, compañías que ofrecen servicios públicos de comunicaciones y otras organizaciones interesadas en temas de comunicación.

Se encarga de supervisar el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos. Por ejemplo, los estándares aseguran que la fabricación de objetos cotidianos, como pueden ser las cámaras fotográficas, se realice de tal forma que dichos objetos puedan usar complementos fabricados en cualquier parte del mundo por empresas ajenas al fabricante original. De éste modo, y siguiendo con el ejemplo de la cámara fotográfica, la gente puede comprar carretes para la misma independientemente del país donde se encuentre y el proveedor del mismo.

**IEEE (Institute Electrical and Electronics Engineers):** es la mayor organización internacional sin ánimo de lucro formada por profesionales de las nuevas tecnologías. Se encarga de elaborar estándares en las áreas de ingeniería eléctrica y computación, como el estándar IEEE 802 para redes de área local o el estándar POSIX para sistemas operativos.

**IETF (Internet Engineering Task Force):** organización creada en los EEUU en 1986 cuyo objetivo principal consiste en desarrollar los estándares que funcionan en Internet. Formada por técnicos y especialistas que publican las recomendaciones de los protocolos de Internet, haciendo que los fabricantes tengan que adaptarse a ellas para evitar problemas de compatibilidad y funcionamiento entre sistemas.

Los documento que publica se denominan RFC y son la base para el desarrollo de todas las tecnologías que funcionan en Internet: RFC 2616 (HTTP), RFC 959 (FTP), RFC 854 (TELNET), etc

## Tema 2 comunicación a través de la red

### 1. Introducción

La comunicación comienza con un mensaje o información que se debe enviar desde una persona o dispositivo a otro. Las personas intercambian ideas mediante diversos métodos de comunicación.

Todos estos métodos tienen tres elementos en común.

El origen del mensaje o emisor. Los orígenes de los mensajes son las personas o los dispositivos electrónicos que deben enviar un mensaje a otras personas o dispositivos.

El destino o receptor del mensaje. El destino recibe el mensaje y lo interpreta.

El canal está formado por los medios que proporcionan el camino por el que el mensaje viaja desde el origen hasta el destino.

### 2. Comunicación de mensajes

En una comunicación simple, como un video musical o un e-mail, puede enviarse a través de la red desde un origen hacia un destino como un **stream de bits** masivo y continuo. Si los mensajes se transmitieran tal cual de esta manera, significaría que ningún otro dispositivo podría enviar o recibir mensajes por la misma red mientras esta transferencia de datos estuviera en progreso. Esperar a que termine el envío de una larga cadena de bits para que otro pueda usar la red mediante unos grandes streams de datos originarían retrasos importantes.

Además, si falla un enlace en la infraestructura de red interconectada durante la transmisión, se perderá todo el mensaje y tendrá que retransmitirse por completo. Un mejor enfoque para enviar datos a través de la red es dividir los datos en partes más pequeñas y más manejables. **La división del stream de datos en partes más pequeñas se denomina segmentación.**

La segmentación de mensajes tiene dos beneficios principales:

**Al enviar partes individuales más pequeñas del origen al destino, se pueden entrelazar diversas conversaciones en la red.** El proceso que se utiliza para entrelazar las piezas de conversaciones separadas en la red se denomina **multiplexación.**

La segmentación puede **aumentar la confiabilidad de las comunicaciones de red.** No es necesario que las partes separadas de cada mensaje sigan el mismo recorrido a través de la red desde el origen hasta el destino. Si una ruta en particular se satura con el tráfico de datos o falla, las partes individuales del mensaje aún pueden direccionarse hacia el destino mediante los recorridos alternativos. Si parte del mensaje no logra llegar al destino, sólo se deben retransmitir las partes faltantes.

### **3. Dispositivos finales**

Los dispositivos de red con los que la gente está más familiarizada se denominan **dispositivos finales.**

Algunos ejemplos de dispositivos finales son:

Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidoresWeb)

Impresoras de red

Teléfonos VoIP

Cámaras de seguridad

Dispositivos móviles de mano (como escáneres de barras inalámbricos, asistentes digitales personales (PDA))

**En el contexto de una red, los dispositivos finales se denominan host.**

Cada host en la red se identifica por una dirección. Cuando un host inicia una comunicación, utiliza la dirección del host de destino para especificar dónde debe ser enviado el mensaje.

### **4. Dispositivos intermediarios**



Las redes dependen de **dispositivos intermediarios** para proporcionar conectividad y para garantizar que los datos fluyan a través de la red.

Estos dispositivos **conectan los hosts individuales a la red** y pueden conectar varias redes individuales para formar una internetwork.

Los siguientes son ejemplos de dispositivos de red intermediarios:

**dispositivos de acceso a la red (hubs, switches y puntos de acceso inalámbricos)**

**dispositivos de internetworking (routers)**

**servidores de comunicación y módems**

**dispositivos de seguridad (firewalls)**

Los dispositivos de red intermediarios realizan las siguientes funciones:

**regenerar y retransmitir** señales de datos

**mantener** información sobre qué rutas existen a través de la red

**notificar** a otros dispositivos los errores y las fallas de comunicación,

**direccionar** datos por rutas alternativas cuando existen fallas en un enlace

**clasificar y direccionar** mensajes según las prioridades de QoS (calidad de servicio)

**permitir o denegar el flujo** de datos en base a configuraciones de seguridad.

## 5. El protocolo de comunicaciones

**Un protocolo es un conjunto de reglas perfectamente organizadas y convenidas de mutuo acuerdo entre los participantes en una comunicación y su misión es regular algún aspecto de la misma.**

Es habitual que los **protocolos** se ofrezcan como normativas o **recomendaciones** de las **asociaciones de estándares**.

Los fabricantes que se ajustan a estas normativas tienen la seguridad de ser compatibles entre sí en aquellos aspectos regulados por el protocolo.

## 6. El concepto de capa o nivel

Con el fin de simplificar la complejidad de cualquier red, **los diseñadores de redes han convenido estructurar las diferentes funciones que realizan y los servicios que proveen en una serie de capas o niveles.**

Las capas están jerarquizadas y cada una se construye sobre su predecesora.

La misión de cada capa es proveer servicios a las capas superiores haciendo transparente el modo en que esos servicios se llevan a cabo.

Así, cada capa debe ocuparse exclusivamente de su nivel inmediatamente inferior a quien solicita servicios y del nivel inmediatamente superior a quien devuelve resultados.

## 7. El interface entre capas

Dos capas consecutivas mantienen relaciones, por lo que es necesario definir el modo en que cada capa negocia los servicios y se comunica con las capas adyacentes.

Llamamos interface de capa a las normas de intercomunicación entre capas.

## 8. La arquitectura de una red

Es el **conjunto organizado de capas y protocolos** de la misma. El diseño de un sistema de comunicación requiere la resolución de muchos y complejos problemas. Por este motivo, **las redes se organizan en capas o niveles** para reducir la complejidad de su diseño.

Cada una de estas capas se construye sobre su predecesor (es decir, utiliza los servicios o funciones diseñados en él) y cada nivel es responsable de ofrecer servicios a las capas superiores.

En una arquitectura por niveles se siguen las siguientes reglas:

- Cada nivel dispone de un conjunto de servicios.
- Los servicios están definidos mediante protocolos estándares
- Cada nivel comunica solamente con el nivel inmediatamente superior y con el inmediatamente inferior.
- Cada uno de los niveles inferiores proporciona servicios a su nivel superior.

### 8.1 Esquema de la estructura del modelo de capas de una arquitectura de red

Las interfaces proporcionan los puntos de acceso a los diferentes servicios que cada capa provee.

La capa N puede solicitar servicios a la capa N-1 y la capa N+1 sólo puede solicitar servicios a la capa N.

La primera capa es una excepción, pues no tiene a quién solicitar servicios, por lo que fundamentalmente se encarga de operar con los medios de transmisión.

Si se cambia algo en la capa N, ninguna otra capa se sentirá afectada siempre que se conserven las estructuras de las interfaces. Principal ventaja de la arquitectura de capas: **es poco sensible a los cambios tecnológicos que se producen por evolución en las funciones y en los servicios de las redes.**

El proceso de comunicación se produce entre las capas equivalentes de dos host distintos.

La información y petición de servicios va descendiendo por la estructura de capas del host emisor hasta que en el nivel más bajo (transmisión física de la señal) la información pasa al host receptor.

A partir de aquí, se inicia el viaje ascendente hasta llegar a la capa equivalente en el host destino de la capa que inició el servicio en el host emisor.

## **9. El modelo de referencia OSI**

**El modelo OSI (Open Systems Interconnection)** está basado en una propuesta establecida en el año 1983 por la organización internacional de normas ISO como un avance hacia la normalización a nivel mundial de protocolos.

Se llama así porque se ocupa de la conexión de sistemas abiertos, es decir, sistemas que están preparados para la comunicación con sistemas diferentes.

**OSI está definido más bien como modelo teórico** y no como arquitectura debido a que la ISO definió la función general que debía realizar cada capa pero no mencionó los servicios y protocolos que se debían usar en cada una de ellas.

### **9.1 Capas del modelo OSI**

El modelo de referencia OSI propone una arquitectura de siete capas o niveles:

NIVEL FÍSICO  
NIVEL DE DATOS  
NIVEL DE RED  
NIVEL DE TRANSPORTE  
NIVEL DE SESIÓN  
NIVEL DE PRESENTACIÓN  
NIVEL DE APLICACIÓN

#### **9.1.1 Nivel o capa física**

Se ocupa de definir las características mecánicas, eléctricas, funcionales y de procedimiento para poder establecer y destruir conexiones entre dos equipos de la red.

En la capa de más bajo nivel, por lo que se ocupa de las transmisiones de los bits. Entre otras funciones debe garantizar:

1. La compatibilidad de los conectores
2. Cuantos pines tiene cada conector y la función de cada uno de ellos.
3. El tipo de sistema de cableado que utilizará
4. La duración de los pulsos eléctricos
5. El número de voltios de cada señal

### 9.1.2 Nivel o capa de enlace

Su misión es **establecer una línea de comunicación libre de errores** que pueda ser utilizada por la capa inmediatamente superior: la capa de red.

Como el nivel físico opera con bits, sin detenerse a averiguar su significado, la capa de enlace debe **fraccionar el mensaje en bloques de datos de nivel 2 o tramas**.

Estas tramas serán enviadas secuencialmente por la línea de transmisión a través de los servicios que ofrece la capa física y quedará a la escucha de las tramas de confirmación que genere la capa de enlace del receptor.

El nivel de enlace se ocupa de tratamiento de los errores que se produzcan en las recepción de las tramas, de eliminar tramas erróneas, solicitar retransmisiones, descartar tramas duplicadas, adecuar el flujo de datos entre emisores rápidos y receptores lentos, etc.

### 9.1.3 Nivel de red

La principal función de este nivel es la del encaminamiento, es decir, cómo elegir la ruta más adecuada para que el bloque de datos del nivel de red o paquete llegue a su destino.

Cada destino está identificado unívocamente en la red por un dirección.

Otra función importante de este capa es el tratamiento de la congestión.

Cuando hay muchos paquetes en la red unos obstruyen a otros generando cuellos de botella.

Otro problema que debe resolver es el que se produce cuando el destinatario de un paquete no está en la misma red, sino en otro, en el que el sistema de direccionamiento es distinto que en la red origen.

En general, la resolución de problemas generados por redes heterogéneas debe resolverse en esta capa.

### 9.1.4 Nivel de transporte

Su misión consiste en aceptar los datos de la capa de sesión, fraccionarlos adecuadamente, de modo que sean aceptables por la subred y asegurarse de que llegarán adecuadamente al nivel de transporte del destinatario.

A este nivel, la conexión es extremo a extremo, no se realiza ninguna conversación con los niveles de transporte de todas las máquinas intermedias.

### **9.1.5 Nivel de sesión**

Permite el diálogo entre emisor y receptor estableciendo una sesión, que es el nombre que reciben las conexiones en esta capa.

Mejora el servicio de la capa de transporte.

Por ejemplo, si transferimos un fichero por una línea telefónica que por su excesivo volumen tardará una hora en efectuar el transporte, y la línea telefónica tiene caídas cada 15 minutos, será imposible transferir el archivo.

La capa de sesión se podría encargar de la resincronización de la transferencia, de modo que en la siguiente conexión se transmitieran datos a partir del último bloque transmitido sin error.

### **9.1.6 Nivel de presentación**

Se ocupa de la sintaxis y de la semántica de la información que se pretende transmitir.

Por ejemplo, si el ordenador emisor utiliza el código ASCII para la representación de información alfanumérica y el ordenador receptor utiliza EBCDIC, no habrá forma de entenderse, salvo que la red provea algún servicio de conversión e interpretación de datos. Esto lo realiza la capa de presentación.

Otra función de la capa de presentación puede ser la de comprimir los datos para que las comunicaciones sean menos costosas o la de encriptación de la información que garantiza la privacidad de la misma.

### **9.1.7 Nivel de aplicación**

Es la capa superior de la jerarquía OSI.

En esta capa se definen los protocolos que utilizarán las aplicaciones y procesos de los usuarios.

Está en contacto directo con los programas o aplicaciones informáticas y contiene los servicios de comunicación más utilizados en las redes.

Por ejemplo, la transferencia de archivos (FTP), el correo electrónico (SMTP), etc.

## **9.2 Comunicación entre dos estaciones**

Los tres primeros niveles (físico, enlace y red) dependen de la red sobre la que funciona, por lo que pueden existir estaciones intermedias en la conversación

Los niveles superiores (transporte, sesión, presentación y aplicación) realizan conversaciones extremo a extremo, es decir, solamente se comunican con las capas de la estación del extremo.

## **9.3 Problema de OSI**

Este modelo no es perfecto, es más, se llega a decir que está mal diseñado debido que algunas capas están prácticamente vacías (es decir, hay muy pocos protocolos definidos dentro de éstas y a la vez son bastante triviales), mientras que otras están llenas a rebosar.

Por ejemplo, la capa de sesión y presentación no se usan en la mayoría de las aplicaciones mientras que las capas inferiores están tan saturadas que en revisiones posteriores se han dividido en múltiples subcapas.

Otro problema es que existen funciones que se repiten en muchas capas, lo que hace que muchos servicios y programas estén duplicados, a la vez que contribuye a un aumento del tamaño de las cabeceras de control de los bloques de información que se transmite.

## **9.4 Transmisión de datos en el modelo OSI**

Observad que en el nivel de enlace se añaden dos encabezados a los datos (al principio y al final). Esto es debido a que la entidad del nivel de enlace debe delimitar los mensajes ya que éstos suelen viajar unos a continuación de los otros por el medio.

Cuando los datos llegan al nivel físico de la máquina receptora, se produce justamente el proceso contrario al anterior, cada capa recibe los datos, le quita su cabecera correspondiente y los pasa al nivel superior.

El nivel de aplicación de la estación A le pasa los datos puros al programa receptor.

## **9.5 Tipos de servicios definidos en OSI**

En OSI existen dos tipos de servicios claramente diferenciados y cada uno provee a la red de una funcionalidad concreta:

**Servicios orientados a conexión:** son servicios que requieren el establecimiento inicial de una conexión y la ruptura o liberación final de la misma. Entre la conexión y la liberación de la misma se produce el intercambio de datos de usuario. Los bloques de datos se reciben en el destino en el mismo orden en que se emitieron en el origen. Todos los paquetes de datos siguen la misma ruta, por lo que los paquetes de datos no necesitan especificar la dirección de destino.

Ejemplo: el servicio telefónico se produce una llamada a un abonado destinatario, se intercambian datos una vez realizada la conexión y se libera la conexión cuando ha acabado la transmisión, dándose por concluida la comunicación.

**Servicios sin conexión:** ofrecen la capacidad de comunicación sin necesidad de realizar una conexión con el destinatario. El emisor envía paquetes al receptor, los cuales deberán de llevar la dirección de destino, y, en algunos casos, el receptor debe enviar acuse de recibo para informarle del éxito de la comunicación.

## 10. Arquitectura TCP/IP

TCP/IP se suele confundir muchas veces con un protocolo de comunicaciones concreto, cuando, en realidad, es una compleja arquitectura de red que incluye varios de ellos, apilados por capas. A día de hoy, es la arquitectura más utilizada ya que es la base de comunicación de Internet.

Motivos de su popularidad:

Es independiente de los fabricantes y marcas comerciales.

Soporta múltiples tecnologías de redes (Ethernet, ATM, Token Ring)

Es capaz de interconectar redes de diferentes tecnologías y fabricantes.

Puede funcionar en máquinas de cualquier tamaño, desde ordenadores personales a grandes supercomputadoras.

Se ha convertido en estándar de comunicación en EEUU desde 1983.

La arquitectura TCP/IP se construyó diseñando inicialmente los protocolos para, posteriormente integrarlos por capas en la arquitectura. Por esta razón, a TCP/IP muchas veces se le califica como pilas de protocolos.

Su modelo es algo diferente a OSI, ya que únicamente existen 4 capas.

### 10.1 Capas TCP/IP

**Capa de subred/acceso a la red:** asimilable a la capa de enlace a la capa física en el modelo OSI. Realiza dos funciones principales: **administración de enlace de datos y transmisión física de datos** en los medios. Los protocolos de administración de enlace

de datos toman los paquetes IP y los formatean para transmitirlos por los medios. Los estándares y protocolos de los medios físicos rigen de qué manera se envían las señales por los medios y cómo las interpretan los clientes que las reciben.

**Capa de internet:** es la más importante y su misión consiste en permitir que las estaciones envíen información (paquetes) a la red y los haga viajar de forma independiente hacia su destino. Durante ese viaje, los paquetes pueden atravesar redes diferentes y llegar desordenados. Esta capa no se responsabiliza de la tarea de ordenar de nuevo los mensajes en el destino.

El protocolo más importante de esta capa se llama IP.

**Capa de transporte:** cumple la función de establecer una comunicación entre el origen y el destino, igual que hace la capa de transporte en el modelo OSI. Puesto que las capas inferiores no se responsabilizan del control de errores ni de la ordenación de los mensajes, ésta debe realizar todo este trabajo. Los protocolos más importantes en esta capa son TCP y UDP.

**Capa de aplicación:** contiene todos los protocolos de alto nivel que utilizan los programas para comunicarse. Aquí se encuentra el protocolo de terminal virtual (TELNET), el de transferencia de archivos (FTP), el protocolo HTTP que usan los navegadores para recuperar páginas web, los protocolos de gestión del correo electrónico, etc.

Las capas de sesión y presentación no existen en la arquitectura TCP/IP ya que los diseñadores pensaron que no eran necesarias.

La experiencia obtenida con los trabajos realizados en el modelo OSI ha comprobado que esta visión fue correcta ya que se utilizaban poco en la mayoría de las aplicaciones de comunicación. En caso de que alguna aplicación desee utilizar un servicio de encriptación de datos o recuperación ante caídas, será necesario incluirlos dentro del propio programa de aplicación.

## **11. Unidad de datos del protocolo y encapsulación**

Mientras los datos de la aplicación bajan al stack del protocolo y se transmiten por los medios de la red, varios protocolos le agregan información en cada nivel. Esto comúnmente se conoce como proceso de encapsulación.

La forma que adopta una sección de datos en cualquier capa se denomina Unidad de datos del protocolo (PDU). Durante la encapsulación, cada capa encapsula las PDU que recibe de la capa inferior de acuerdo con el protocolo que se utiliza.



En cada etapa del proceso, una PDU tiene un nombre distinto para reflejar su nuevo aspecto:

1. Datos: el término general para las PDU que se utilizan en la capa de aplicación.
2. Segmento: PDU de la capa de transporte.
3. Paquete: PDU de la capa de Internetwork.
4. Trama: PDU de la capa de acceso a la red.
5. Bits: una PDU que se utiliza cuando se transmiten físicamente datos a través de un medio.

## **12. Direccionamiento en la red**

Es muy importante que cada parte de los datos contenga suficiente información de identificación para llegar al destino correcto. Existen varios tipos de direcciones que deben incluirse para entregar satisfactoriamente los datos desde una aplicación de origen que se ejecuta en un host hasta la aplicación de destino correcta que se ejecuta en otro.

FISICA: bits de sincronización

ENLACE: direcciones físicas de origen y destino ( MAC )

RED: Direcciones de red lógicas de origen y destino ( IP )

TRANSPORTE: número de proceso de origen y destino ( Puertos )

CAPAS SUPERIORES: Datos de aplicaciones codificados.

## **13. Proceso de envío y recepción**

Ver animación 2.4.6

## **14. Envío de datos a la aplicación correcta**

En el dispositivo final, el número de puerto de servicio dirige los datos a la conversación correcta.

# **TEMA3.- Sistema de cableado estructurado y espacios físicos de una red**

## **1. La capa física**

La capa física de OSI proporciona los medios de transporte para los bits que conforman la trama de la capa de Enlace de datos a través de los medios de red.

Esta capa acepta una trama completa desde la capa de Enlace de datos y lo codifica como una secuencia de señales que se transmiten en los medios locales.

El objetivo de la capa física es crear la señal óptica, eléctrica o de microondas que representa a los bits en cada trama.

Luego, estas señales se envían por los medios una a la vez.

Otra función de la capa física es la de recuperar estas señales individuales desde los medios, restaurarlas para sus representaciones de bit y enviar los bits hacia la capa de Enlace de datos como una trama completa.

## **2. Capa física. Funcionamiento**

Cuando se diseña una red de transmisión de datos hay que tener en cuenta el medio empleado para comunicar los equipos.

A esta parte de la red que se encarga de transportar la información de un origen a un destino se le denomina medio de transmisión.

El medio de transmisión está relacionado directamente con los protocolos de nivel físico de la arquitectura de la red y es el encargado de hacer efectivo el transporte de la información.

Sin embargo, a parte del medio de transmisión, se hace necesaria una “logística” que lo apoye.

Existen tres tipos básicos de medios de red en los cuales se representan los datos:

- Cable de cobre
- Fibra
- Inalámbrico

La presentación de los bits -es decir, el tipo de señal- depende del tipo de medio.

Para los medios de cable de cobre, las señales son patrones de pulsos eléctricos.

Para los medios de fibra, las señales son patrones de luz.

Para los medios inalámbricos, las señales son patrones de transmisiones de radio.

## **3. Capa física. Estándares**

La capa física consiste en un hardware creado por ingenieros en forma de conectores, medios y circuitos electrónicos.

Por lo tanto, es necesario que las principales organizaciones especializadas en ingeniería eléctrica y en comunicaciones definan los estándares que rigen este hardware.

Los estándares para la capa física especifican los requisitos de cableado, conectores y señales

Por el contrario, las operaciones y los protocolos de las capas superiores de OSI se llevan a cabo mediante un software y están diseñados por especialistas informáticos e ingenieros de software.

## 4. Métodos de señalización

Para poder realizar el transporte de la información, los protocolos del nivel físico deben tener en cuenta muchas cuestiones de fondo:

¿de qué manera se envían los dígitos binarios por el medio?

¿cómo se corrigen las distorsiones y perturbaciones que sufre la señal en su camino?

¿qué medio de transmisión resulta más adecuado para el envío de la información?

Para que la información pueda transmitirse por un determinado medio (el aire, cables de cobre, etc) es necesario convertir de alguna forma esos ceros y unos para que puedan viajar hasta el receptor y éste pueda interpretarlos correctamente.

Dentro de un ordenador, los dígitos binarios se transmiten de unos dispositivos a otros como señales eléctricas.

A cada dígito binario se le puede asociar un nivel de tensión o voltaje diferente, por ejemplo, un valor de +5 voltios para representar un 1 y 0 voltios para representar un 0. Los circuitos de un ordenador interpretan un 1 cuando por la conexión correspondiente reciben corriente eléctrica (cuya tensión se aproxima a los 5 voltios), mientras que interpretan un 0 cuando no hay corriente.

El funcionamiento de los circuitos digitales es análogo al de una bombilla: cuando se enciende, podemos tomarlo como un 1 y cuando está apagado, como un 0.

Solamente se encenderá la bombilla cuando circule corriente eléctrica a través de ella.

Suele considerarse que la transmisión de las señales por los cables suele ser perfecta. Sin embargo, en la realidad no ocurre así debido a la tecnología utilizada para fabricar los componentes.

Esto implica que los circuitos digitales deben asignar rangos en vez de niveles de tensión exacta para poder interpretar la información.

### 4.1 Características de las señales

Los bits se representan en el medio al cambiar una o más de las siguientes características de una señal: amplitud, frecuencia ó fase.

Una señal viene definida por tres características:

**Amplitud:** es el valor máximo de la señal en un intervalo

**Frecuencia:** determina el número de veces que la señal se repite por segundo (medida en Hertzios)

**Fase:** indica el intervalo de tiempo que va desde el instante inicial al primer punto donde la señal toma valor cero.

## 5. Capacidad para transportar datos

Los diferentes medios físicos admiten la transferencia de bits a distintas velocidades. La transferencia de datos puede medirse de tres formas:

**Ancho de banda**

**Rendimiento**

**Capacidad de transferencia útil**

**Ancho de banda:** El ancho de banda digital mide la cantidad de información que puede fluir desde un lugar hacia otro en un período de tiempo determinado. El ancho de banda generalmente se mide en kilobits por segundo (kbps) o megabits por segundo (Mbps).

**Rendimiento:** El rendimiento es la medida de transferencia de bits a través de los medios durante un período de tiempo determinado. Debido a diferentes factores, el rendimiento generalmente no coincide con el ancho de banda.

Por ejemplo, en una internetwork el rendimiento no puede ser más rápido que el enlace más lento de la ruta de origen a destino. Incluso si todos los segmentos o gran parte de ellos tienen un ancho de banda elevado, sólo se necesita un segmento en la ruta con un rendimiento inferior para crear un cuello de botella en el rendimiento de toda la red.

Capacidad de transferencia útil: es la medida de datos utilizables transferidos durante un período de tiempo determinado. Por lo tanto, es la medida de mayor interés para los usuarios de la red. La capacidad de transferencia útil mide la transferencia efectiva de los datos del usuario entre las entidades de la capa de aplicación, por ejemplo entre el proceso de un servidor Web de origen y un dispositivo con exploradorWeb de destino.

A diferencia del rendimiento, que mide la transferencia de bits y no la transferencia de datos utilizables, la capacidad de transferencia útil considera los bits que generan la sobrecarga del protocolo.

Esta capacidad representa el rendimiento sin la sobrecarga de tráfico para establecer sesiones, acuses de recibo y encapsulaciones.

Por ejemplo, considere dos hosts en una LAN que transfiere un archivo. El ancho de banda de la LAN es de 100 Mbps. Debido al uso compartido y al encabezado de los medios, el rendimiento entre los equipos es solamente de 60 Mbps. Con una sobrecarga del proceso de encapsulación de stack TCP/IP, la velocidad real de los datos recibidos por

la computadora de destino, es decir la capacidad de transferencia útil, es sólo de 40 Mbps.

## **6. Medios de transmisión**

El medio de transmisión es el soporte físico que facilita el transporte de la información y supone una parte fundamental en la comunicación de datos.

Dos tipos de medios:

Guiados: conducen las ondas a través de un campo físico (cables)

No guiados: proporcionan un soporte para que las ondas se transmitan, pero no las dirigen (el aire)

La naturaleza del medio junto con la de la señal que se transmite a través de él, constituye un factor determinante de las características y la calidad de la transmisión.

### **6.1 Medios de cobre**

El medio más utilizado para las comunicaciones de datos es el cableado que utiliza alambres de cobre para señalar bits de control y datos entre los dispositivos de red.

Los datos se transmiten en cables de cobre como impulsos eléctricos.

#### **6.1.1 Par sin trenzar (paralelo)**

Está formado por dos hilos de cobre paralelos recubiertos de un material aislante (plástico).

Ofrece muy poca protección frente a las interferencias.

Las conexiones se realizan mediante un conector denominado RJ-11.

Usos:

Se suele utilizar como cable telefónico para transmitir voz analógica.

En tendido eléctrico de alta tensión

Transmisión de datos a corta distancia (apenas unos metros) dentro del ordenador para comunicar entre sí los diferentes elementos internos dentro de él, debido a que la distancia que los separa es muy corta)

Según los estándares del cableado, a este tipo de cable se le conoce como cable de categoría 1.

#### **6.1.1 Par sin trenzar (paralelo) II**

#### **6.1.2. Par trenzado**

Consiste en dos cables de cobre aislados enlazados de dos en dos de forma helicoidal, semejante a la estructura del ADN.

El objetivo del trenzado del cable es reducir la interferencia eléctrica y otras interferencias del exterior.

Debido a su fácil instalación, velocidad de transmisión de hasta varios Mbps y bajo coste, los pares trenzados se utilizan ampliamente y se seguirán utilizando por mucho tiempo.

Existen dos tipos:

Pares trenzados no apantallados (UTP ó Unshielded Twisted Pair): consiste en cuatro pares de alambres codificados por color que han sido trenzados y cubiertos por un revestimiento de plástico flexible sin recubrimiento metálico externo, de modo que es muy sensible a las interferencias. Cable barato, flexible y sencillo de instalar.

Concepto a revisar: Crosstalk

Pares trenzados apantallados (STP ó Shielded Twisted Pair): semejante al anterior pero se le añade un recubrimiento metálico para evitar las interferencias externas. Es un cable más protegido pero menos flexible que el UTP.

Tiene más ventajas eléctricas que el cable UTP por lo que, en principio, siempre se tendría que elegir STP en vez de UTP. Sin embargo, la falta de flexibilidad debido a su rigidez, hace que sólo se utilice donde realmente hace falta: en entornos eléctricamente hostiles.

#### 6.1.2.1 Clasificaciones del par trenzado

En los cables de pares hay que distinguir dos clasificaciones:

Las categorías: especifica unas características eléctricas para el cable como atenuación, capacidad de la línea e impedancia (oposición al paso de la corriente alterna). Las categorías 3 a 5 que soportan frecuencias de 10, 20 y 100 MHz respectivamente empiezan a estar en desuso aunque aún se encuentran en instalaciones antiguas.

También se utiliza una categoría llamada 5e que mejora las capacidades de la categoría 5. Las categorías 6 y 7 llegan a transmisiones de 250 y 600 MHz respectivamente. La categoría 7 tiene como competidor más directo a la fibra óptica.

Actualmente lo más frecuente es instalar categoría 5e y 6.

Las clases: cada clase especifica las distancias permitidas, el ancho de banda conseguido y las aplicaciones para las que es útil en función de estas características.

Tabla 4.1. Características de longitudes posibles y anchos de banda para las clases y categorías de pares trenzados

### 6.1.2.1 Clasificaciones del par trenzado (III)

Dado que el cable UTP 5 y 5e es barato y fácil de instalar se utiliza habitualmente en las instalaciones de redes de área local con topología en estrella.

### 6.1.2.2 Tipos de cable UTP

El cableado UTP que se encuentra comúnmente en el trabajo, las escuelas y los hogares cumple con los estándares estipulados en conjunto por la Asociación de las Industrias de las Telecomunicaciones (TIA) y la Asociación de Industrias Electrónicas (EIA).

TIA/EIA-568A estipula los estándares comerciales de cableado para las instalaciones LAN y es el estándar de mayor uso en entornos de cableado LAN.

Estos cables se construyen de acuerdo con la normal T568A ó la T568B.

Siempre se recomienda utilizar preferentemente la norma T568A aunque lo más importante es seguir siempre la misma norma en una instalación para evitar posibles errores o problemas.

Existen dos tipos de latiguillos RJ45:

Cables cruzados: utilizados para comunicar dispositivos que funcionan en el mismo nivel de arquitectura (por ejemplo, para conectar dos conmutadores o dos estaciones). En resumen, los cables de conexión cruzada conectan directamente los siguientes dispositivos en una LAN:

Switch a switch

Switch a hub

Hub a hub

Router a conexión del puerto Ethernet del router

Equipo a equipo

Equipo a puerto Ethernet del router

Para la construcción de cables cruzados se engasta cada extremo utilizando un estándar diferente (uno será 568A y el otro 568B). Esto es así para que el terminal transmisor de uno de los dispositivos necesita conectarse al terminal receptor del otro dispositivo.

El cable debe tener una terminación para que el pin transmisor, Tx, que toma la señal desde el dispositivo A en un extremo, se conecte al pin receptor, Rx, en el dispositivo B. De manera similar, el pin Tx del dispositivo B debe estar conectado al pin Rx del dispositivo A. Si el pin Tx de un dispositivo tiene el número 1 y el pin Rx tiene el número 2, el cable conecta el pin 1 en un extremo con el pin 2 en el otro extremo.

Cables directos: sirve para conectar dispositivos desiguales, como un computador con un hub o switch. En este caso ambos extremos del cable deben tener la misma distribución.

No existe diferencia alguna en la conectividad entre la distribución 568B y la distribución 568A siempre y cuando en ambos extremos se use la misma.

En definitiva, se utilizan cables directos para las siguientes conexiones:

- Switch a puerto Ethernet del router
- Equipo a switch
- Equipo a hub

Cada vez que se realiza la terminación de un cableado de cobre, existe la posibilidad de que se pierda la señal y de que se genere ruido en el circuito de comunicación.

Cuando se realizan las terminaciones de manera incorrecta, cada cable representa una posible fuente de degradación del funcionamiento de la capa física.

Es fundamental que todas las terminaciones de medios de cobre sean de calidad superior para garantizar un funcionamiento óptimo con tecnologías de red actuales y futuras.

En una LAN Ethernet, los dispositivos utilizan uno de los dos tipos de interfaces UTP: MDI o MDIX.

La MDI (interfaz dependiente del medio) utiliza un diagrama de pines normal de Ethernet. Los pines 1 y 2 se utilizan como transmisores y los pines 3 y 6 como receptores. Dispositivos como computadoras, servidores o routers tendrán conexiones MDI.

Los dispositivos que proporcionan la conectividad a la LAN (por lo general, hubs o switches) habitualmente utilizan conexiones MDIX (Interfaz cruzada dependiente del medio). Los cables MDIX intercambian los pares transmisores internamente. Este intercambio permite que los dispositivos finales se encuentren conectados a un hub o switch utilizando un cable de conexión cruzado.

Una gran cantidad de dispositivos permite que el puerto Ethernet UTP se establezca en MDI o en MDIX.

Esta configuración puede realizarse en una de tres formas, según las características del dispositivo:

1. En algunos dispositivos, los puertos pueden incluir un mecanismo que intercambia de manera eléctrica los pares receptores y transmisores. El puerto puede cambiarse de MDI a MDIX al activar el mecanismo.
2. Como parte de la configuración, algunos dispositivos permiten seleccionar la función del puerto como MDI o MDIX.
3. Muchos de los dispositivos más nuevos incluyen una característica de conexión cruzada automática. Esta característica permite al dispositivo detectar el tipo de cable requerido y configura las interfaces según corresponda. En algunos dispositivos, esta detección automática se realiza en forma predeterminada. Otros dispositivos que requieren un comando de configuración de interfaz para habilitar la detección automática de MDIX.



### 6.1.3 Cable coaxial

Consta de un alambre de cobre duro en su parte central por donde circula la señal, el cual se encuentra rodeado por un material aislante.

Este material está rodeado por un conductor cilíndrico presentado como una malla de cobre trenzado. A su vez, el conductor externo está cubierto por una capa de plástico protector. Esta construcción le confiere una excelente inmunidad al ruido.

Solían utilizarse en el sistema telefónico como conexiones de gran capacidad y largo recorrido pero ahora se ha reemplazado por la fibra óptica. Aún se utiliza para la televisión por cable y para acceso a redes de área extensa.

## 6.2 Fibra óptica

El cableado de fibra óptica utiliza fibras de plástico o de vidrio para guiar los impulsos de luz desde el origen hacia el destino. Los bits se codifican en la fibra como impulsos de luz. El cableado de fibra óptica puede generar velocidades muy superiores de ancho de banda para transmitir datos sin procesar.

Un sistema de transmisión óptico tiene tres componentes:

- A. La fuente de luz: se encarga de convertir una señal digital en una señal óptica. Típicamente se utiliza un pulso de luz para representar un 1 y la ausencia de luz para representar un 0.
- B. El medio de transmisión: es una fibra de vidrio ultradelgada que transporta la luz.
- C. El detector: se encarga de generar un pulso eléctrico en el momento en el que la luz incide sobre él.

El cable de fibra óptica consta de un núcleo, un revestimiento y una cubierta externa protectora.

El núcleo es el conductor de la señal luminosa. La señal es conducida por el interior de este núcleo fibroso.

El revestimiento tiene como objetivo mantener toda la luz en el interior de él. La cubierta sirve para proteger el revestimiento e impedir que cualquier rayo de luz del exterior penetre en la fibra.

### 6.2.1 Tipos de fibra óptica

En términos generales, los cables de fibra óptica pueden clasificarse en dos tipos: monomodo y multimodo.

**Monomodo:** la fibra es tan delgada que la luz se transmite en línea recta. Transporta un sólo rayo de luz, generalmente emitido desde un láser. Este tipo de fibra puede transmitir

impulsos ópticos en distancias muy largas, ya que la luz del láser es unidireccional y viaja a través del centro de la fibra.

**Multimodo:** la luz se transmite por el interior del núcleo incidiendo sobre su superficie interna, como si se trata de un espejo. La fibra óptica multimodo a menudo utiliza emisores LED que no generan una única ola de luz coherente. La luz de un LED ingresa a la fibra multimodo en diferentes ángulos.

La fibra multimodo y la fuente de luz del LED que utiliza resultan más económicas que la fibra monomodo y su tecnología del emisor basada en láser.

## 6.2.2 Ventajas e inconvenientes

Con la tecnología actual, la fibra óptica permite velocidades mayores que el resto de medios de transmisión (el límite para alcanzar más velocidad se encuentra en la incapacidad que los dispositivos tienen para convertir con mayor rapidez las señales eléctricas a ópticas y al revés).

Permite instalar cables de longitudes muy elevadas (hasta 30km) aunque una baja calidad en la fabricación de la fibra puede hacer que las impurezas que contenga absorban parte de la señal, lo que puede limitar sus longitudes máximas.

Algunos de los problemas de implementación de medios de fibra óptica:

Más costoso (comúnmente) que los medios de cobre en la misma distancia (pero para una capacidad mayor)

Se necesitan diferentes habilidades y equipamiento para terminar y empalmar la infraestructura de cables

Manejo más cuidadoso que los medios de cobre

En la actualidad, en la mayor parte de los entornos empresariales se utiliza principalmente la fibra óptica como cableado backbone para conexiones punto a punto con una gran cantidad de tráfico entre los servicios de distribución de datos y para la interconexión de los edificios en el caso de los campus compuestos por varios edificios.

Ya que la fibra óptica no conduce electricidad y presenta una pérdida de señal baja, es ideal para estos usos.

## 6.2.4 Fibra óptica vs Cables de cobre

Las ventajas de la fibra frente a los cables de cobre son:

Puede manejar anchos de banda mucho más grandes que el cobre.

Debido a su baja atenuación, sólo se necesitan repetidores cada 30 km (en el cobre se necesitan repetidores cada 5 km).

Teniendo en cuenta que las fibras utilizadas en los medios de fibra óptica no son conductores eléctricos, este medio es inmune a la interferencia electromagnética.

Es delgada y ligera

No tienen fugas y es muy difícil intervenirlas.

### **6.3 Medios inalámbricos**

La comunicación inalámbrica prescinde de cualquier cable entre el emisor y el receptor. Resulta útil para usuarios móviles que tienen que estar continuamente conectados y cuando resulta costoso tender hilos de comunicación en zonas geográficas de difícil acceso.

Consisten en el envío y recepción de electrones que circulan por el espacio libre (aire). Estas partículas viajan en forma de ondas electromagnéticas que se propagan de la misma forma que las ondas en un estanque.

Las tecnologías inalámbricas de comunicación de datos funcionan bien en entornos abiertos. Sin embargo, existen determinados materiales de construcción utilizados en edificios y estructuras, además del terreno local, que limitan la cobertura efectiva.

El medio inalámbrico también es susceptible a la interferencia y puede distorsionarse por dispositivos comunes como teléfonos inalámbricos domésticos, algunos tipos de luces fluorescentes, hornos microondas y otras comunicaciones inalámbricas.

Los dispositivos y usuarios que no están autorizados a ingresar a la red pueden obtener acceso a la transmisión, ya que la cobertura de la comunicación inalámbrica no requiere el acceso a una conexión física de los medios.

Por lo tanto, la seguridad de la red es el componente principal de la administración de redes inalámbricas.

#### **6.3.1 LAN inalámbrica**

Una implementación común de transmisión inalámbrica de datos permite a los dispositivos conectarse en forma inalámbrica a través de una LAN.

En general, una LAN inalámbrica requiere los siguientes dispositivos de red:

Punto de acceso inalámbrico (AP): Concentra las señales inalámbricas de los usuarios y se conecta, generalmente a través de un cable de cobre, a la infraestructura de red existente basada en cobre.

Adaptadores NIC inalámbricos: Proporcionan capacidad de comunicación inalámbrica a cada host de la red.

Los beneficios de las tecnologías inalámbricas de comunicación de datos son evidentes, especialmente en cuanto al ahorro en el cableado costoso de las instalaciones y en la conveniencia de la movilidad del host.

Sin embargo, los administradores de red necesitan desarrollar y aplicar procesos y políticas de seguridad rigurosas para proteger las LAN inalámbricas del daño y el acceso no autorizado.

## 7. Cableado estructurado

La instalación de un red suele seguir una serie de normas que aseguran un buen funcionamiento y permiten que la administración no se convierta en un quebradero de cabeza cuando es necesario realizar una ampliación ó mantener la red por la ruptura de algún cable o conector.

Un estándar de cableado estructurado especifica cómo debe organizarse la instalación del cableado de comunicaciones en edificios, sobre todo, a nivel empresarial.

El estándar especifica de forma concisa el tipo de cable a utilizar, conectores, longitudes máximas de los tramos, organización de los elementos de interconexión, etc.

### 7.1 Elementos del cableado estructurado

Un sistema de cableado bien diseñado debe tener al menos estas dos cualidades: seguridad y flexibilidad.

A estos parámetros se le pueden añadir otros menos importantes como son el coste económico, la facilidad de la instalación, etc.

Podemos definir el cableado estructurado como una técnica que permite cambiar, identificar, mover periféricos o equipos de una red con flexibilidad y sencillez.

La estructuración del cable se consigue construyendo módulos independientes que segmenten la red en subsistemas de red, independientes pero integrados.

Estos subsistemas siguen una organización jerarquizada por niveles, desde el sistema principal hasta el último de los subsistemas.

Partiendo del subsistema de más alto nivel tenemos la siguiente organización:

**Cableado de campus:** se utiliza para interconectar los diferentes edificios de la organización. Puesto que por éste circula gran cantidad de tráfico, se recomienda el uso de fibra óptica.

**Entrada del edificio:** es el punto en el que se conectan los cables exteriores con los cables interiores del edificio. Es la frontera que separa la instalación que es responsabilidad de la compañía de comunicaciones con la instalación privada gestionada por la empresa. También conocido como punto de demarcación o demarc.

**Sala de equipamiento:** es el punto en el que confluyen todas las conexiones del edificio, por lo que su complejidad de montaje es mayor que la de cualquier otra sala.

**Cableado vertical o backbone:** es el encargado de comunicar todos los subsistemas horizontales, por lo que requiere medios de transmisión con un ancho de banda elevado y elevada protección.

**Armario de distribución:** es el lugar en el que confluyen los cables de comunicaciones. Contienen todos los concentradores (hubs) de cableado, conmutadores (switchs), puentes, etc montados en los armarios en rack y conectados mediante paneles de distribución.

Un **rack** es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones.

Las medidas para la anchura están normalizadas para que sean compatibles con equipamiento de cualquier fabricante. También son llamados bastidores ó cabinas.

**Cableado horizontal o de planta:** se extiende desde las conexiones de pared (rosetas) de las oficinas y despachos hasta los armarios de comunicaciones.

**Área de trabajo:** es el punto de conexión entre los dispositivos (pcs) y los enchufes de pared. Los cables que conectan los enchufes de pared con los equipos deben tener una calidad mínima igual a la del cableado horizontal al que están conectados.

## 7.2 Longitudes máximas de cable de cobre

Las longitudes máximas depende de la longitud del cableado horizontal. Si se reduce su longitud, entonces se puede aumentar la longitud del cableado del área de trabajo o los latiguillos de los paneles.

Para cableado de fibra óptica se permiten longitudes mayores y cualquier combinación es aceptada por los estándares siempre que la longitud total del cable horizontal más el cable del área de trabajo no exceda los 100m.

## 7.3 Dispositivos de conexión de cables

Los cables que forman parte de una red de transmisión de datos no pueden utilizarse si la señal eléctrica no entra en ellos debidamente.

De esta función se ocupan los conectores, que son los interfaces que adecuan la señal de cable al interfaz del receptor.

En una LAN, los conectores conectan los cables a las tarjetas de red.

Algunos de estos conectores son:

**RJ11, RJ12 y RJ45:** Estos conectores se utilizan con cables UTP y STP y otros cables de pares. RJ11 y RJ12 se utilizan mayoritariamente para enlazar redes de telefonía y RJ45 como interfaz física para conectar redes de cableado estructurado

**BNC:** se utiliza con cable coaxial. Hoy en día, se utilizan muchísimo en sistemas de televisión y vídeo.

**SC y ST:** son los conectores utilizados en las instalaciones de fibra óptica. Se diferencian en que el ST requiere un giro del conector para la inserción del mismo mientras que los SC son de conexión directa. Además, el ST suele utilizarse en instalaciones híbridas entre cables de pares y fibra óptica. SC monomodo y ST multimodo

**Conector Lucent (LC):** un conector pequeño que está adquiriendo popularidad en su uso con fibra monomodo; también admite la fibra multimodo.

**Patch panels:** es un dispositivo de interconexión encargado de recibir todos los cables del cableado estructurado. Sirve como un organizador de las conexiones de la red, para que los elementos relacionados de la Red LAN y los equipos de la conectividad puedan ser fácilmente incorporados al sistema.

## 7.5 Herramientas utilizadas en la conectorización

La creación de las conexiones de la red debe realizarse con sumo cuidado ya que la mayor parte de los problemas de las redes de área local una vez que han entrado en funcionamiento se relacionan directamente con problemas en los cables o en los conectores.

Las herramientas utilizadas en la construcción de las conexiones de cableado dependerán del tipo de cable y de conector.

De forma general, suelen utilizarse alicates, cuchillas y **crimpadoras**. Se denomina crimpar, grimpar, ponchar y punchar la acción del alicate compresor que integra los filamentos del cable de cobre con las cuchillas de cada pin en el conector.

Otros componentes que mejoran la calidad de la instalación: bridas y etiquetas identificativas.

## 7.6 Etiquetado de cables

La norma EIA/TIA-606 especifica que cada terminación de hardware debe tener alguna etiqueta que lo identifique de forma exclusiva.

Un cable tiene dos terminadores, por tanto, cada uno de estos extremos recibirá un nombre.

No es recomendable la utilización de un sistema de etiquetado con relación a un momento concreto, es mejor utilizar nomenclaturas neutras. Ejemplo: si etiquetamos un PC como PC de Dirección y luego el lugar del edificio en donde se ubica la Dirección cambia, tendríamos que cambiar también el etiquetado.

Se recomienda la utilización de etiquetas que incluyan un identificador de sala y un identificador de conector y así sabremos todo sobre el cable: dónde empieza y dónde acaba.

Ejemplo: 03RS02-05RS24 Este cable indica que está tendido desde la roseta 2 de la sala 03 hasta la roseta 24 de la sala 5. Las rosetas en las salas 3 y 5 irían etiquetadas con 03RS02 y 05RS24 respectivamente.

## 7.7 Elementos de la instalación

La instalación de la red no sólo se compone de cables y conectores.

Estos deben de ser fijados a las instalaciones de los edificios y además hay que hacerlos convivir con otras instalaciones de otra naturaleza que probablemente hayan sido tendidas con anterioridad: agua, electricidad, aire acondicionado, etc.

Para realizar una buena instalación de la red se utilizan los siguientes elementos:

**Balums y transceptores:** adaptan la señal pasándola de coaxial a UTP ó, en general, a cables de pares sean o no trenzados. Su utilización produce pérdidas de señal ya que deben adaptar la impedancia de un tipo de cable a otro.

**Armarios (racks):** En instalaciones de tipo medio o grande, los equipos de comunicaciones se instalan en armarios especiales que tienen unas dimensiones estandarizadas y en los que es fácil su manipulación y la fijación de los cables que a ellos se conectan.

Dentro de estos armarios o racks se instalan bandejas de soporte o patch panel para la conexión de los conectores. La altura de los armarios suele medirse en U.

**Latiguillos:** cables cortos utilizados para prolongar los cables entrantes o salientes del rack.

**Canaletas:** Son los conductos a través de los cuales se tienden los cables que quedan recogidos y protegidos convenientemente. Hay canaletas decorativas, de aspecto más acabado cuya misión es ocultar los cables, y canaletas acanaladas que suelen instalarse en los falsos techos o falsos suelos y que son suficientemente grandes como para llevar muchos cables.

**Rosetas:** conectores que se insertan en las canaletas o se adosan en la pared y que sirven de interface entre el latiguillo que lleva la señal al nodo y el cable de red.

**Suelos y techos técnicos:** Las canalizaciones tendidas por suelos y techos técnicos mejoran la limpieza de la instalación haciéndola mucho más estética. Los cables llegan a los armarios a través de los falsos suelos justo por debajo de ellos, lo que ayuda a la limpieza de la instalación. Los distintos cables avanzan ordenadamente, normalmente embreados, por los vértices del armario hasta alcanzar la altura a la que deben de ser conectados en algún dispositivo del patch panel.

## 7.8 Certificación de la instalación

La certificación de una instalación de cableado se utiliza para comprobar que es adecuada para las necesidades de comunicación de la organización, es decir, que permite comprobar que el rendimiento que ofrece se corresponde con el presupuestado.

También permite comprobar que todas las conexiones se han realizado correctamente y que no existen cables mal instalados.

La certificación del cableado se realiza utilizando aparatos portátiles que miden los parámetros más importantes del cableado: diafonía (Perturbación electromagnética producida en un canal de comunicación por el acoplamiento de este con otro u otros vecinos), atenuación y longitud.

Estos aparatos se denominan genéricamente comprobadores de red.

Los dispositivos de comprobación de red están disponibles para cable de par trenzado con y sin apantallar, cable coaxial y fibra óptica.

Existen tres tipos de comprobadores básicos:

**Comprobadores de continuidad:** se dedican a comprobar si los cables están bien montados o tienen algún corte. Son dispositivos muy sencillos y de un coste reducido, y se limitan a comprobar su cada uno de los hilos del cable ofrece continuidad o está cortado.



**Comprobadores de cableado:** son más avanzados que los anteriores puesto que aparte de realizar comprobaciones de continuidad, son capaces de realizar comprobaciones de diafonía, atenuación y ruido.

Reflector de Dominio del Tiempo (TDR): son los más avanzados y de mayor coste ya que pueden realizar comprobaciones como detección de empalmes, nudos, radios de curvatura del cable demasiado pronunciados, etc. Los comprobadores para fibra óptica llamados OTDR pueden calcular la atenuación del fragmento de cable y las pérdidas en los conectores. Además de detectar las anomalías indican en qué punto de la línea se están produciendo.

Los TDR son capaces de indicar en qué punto del cable (contando la distancia desde el extremo en el que se encuentra el comprobador) está localizada la avería.

Esto se consigue gracias a que una pequeña parte de la señal que circula por el cable rebota en el lugar donde existe alguna anomalía y vuelve a su extremo de origen. Si se mide el tiempo que tarda la señal en volver al origen después de haber rebotado, entonces se puede calcular a qué distancia se encuentra esa anomalía.

Para realizar la comprobación de un fragmento de cable hay que colocar el aparato en un extremo del cable, mientras que en el otro se conecta una sonda o unidad remota que va incluida en el aparato.

Para facilitar en un futuro la localización de problemas o averías en la red, se recomienda que se anoten y se conserven todos los valores obtenidos durante la fase de certificación de la red.

## **7.9 El proyecto de instalación**

La instalación consiste en la ejecución ordenada de un conjunto de tareas que revierten en proporcionar el servicio que el cliente que solicitó la instalación necesitaba.

Algunas de estas tareas son:

Instalación de las tomas de corriente: esta tarea suele realizarla un electricista y nuestra tarea consiste en asegurarnos que existen tomas de corriente para alimentar todos los equipos de comunicaciones.

Instalación de rosetas y jacks: es la instalación de los puntos de red finales desde los que se conectarán los equipos de comunicaciones sirviéndose de latiguillos.

Tendido de los cables: se trata de medir la distancia que debe recorrer cada cable y añadirle una longitud prudente que nos permita trabajar cómodamente con él antes de cortarlo.

Conectorización de los cables en los patch panels y en las rosetas: utilizando las herramientas de crimpado apropiadas. A esto se le denomina cross-connect.

Probado de los cables instalados: cada cable construido y conectorizado debe ser inmediatamente probado para asegurarse de que cumplirá correctamente su función.

Etiquetado y documentación del cable y conectores: todo cable debe ser etiquetado en ambos extremos así como los conectores de patch panels y rosetas de modo que queden identificado unívocamente.

Instalación de los adaptadores de red: en caso de que los equipos no lleven la tarjeta de red instalada, habrá que instalarla.

Instalación de los dispositivos de red: se trata de instalar los concentradores, conmutadores, puentes y encaminadores.

Configuración del software de red en clientes y servidores de la red

## TEMA 4 Nivel de enlace

### 1. Introducción

Para que los paquetes de capa de red sean transportados desde el host origen al host destino deben recorrer diferentes redes físicas.

Estas redes físicas pueden componerse de diferentes tipos de medios físicos, tales como alambres de cobre, microondas, fibras ópticas y enlaces satelitales.

Los paquetes de capas de red no tienen una manera de acceder directamente a los diferentes medios físicos (cobre, fibra óptica, etc).

La función de la capa de enlace de datos de OSI es preparar los paquetes de la capa de red para ser transmitidos y controlar el acceso a los medios físicos.

### 2. La capa de enlace

La capa de enlace de datos realiza dos servicios básicos:

Permite a las capas superiores acceder a los medios usando técnicas, como **tramas**.

Controla cómo los datos se ubican en los medios y son recibidos desde los medios usando técnicas como **control de acceso** a los medios y **detección de errores**.

Existen términos específicos para esta capa:

**Trama:** la PDU de la capa de enlace de datos.

**Nodo:** la notación de la Capa 2 para dispositivos de red conectados a un medio común.

**Medios/medio (físico):** los medios físicos para la transferencia de información entre dos nodos.

**Red (física):** dos o más nodos conectados a un medio común.

La capa de enlace de datos es responsable del intercambio de tramas entre nodos a través de los medios de una red física.

### 3. PDU de la capa de enlace

La PDU de la capa de enlace recibe el nombre de **trama**.

La trama de la capa de enlace de datos incluye:

**Datos:** El paquete desde la Capa de red

**Encabezado:** contiene información de control como direccionamiento y está ubicado al comienzo del PDU

**Tráiler:** contiene información de control para detección de errores agregada al final del PDU

A pesar de que hay muchos protocolos de capa de enlace de datos diferentes que describen las tramas de la capa de enlace de datos, cada tipo de trama tiene las tres partes básicas comentadas: Encabezado, datos, y tráiler.

Todos los protocolos de capa de enlace de datos encapsulan la PDU de la capa 3 dentro del campo de datos de la trama.

Sin embargo, la estructura de la trama y los campos contenidos en el encabezado y tráiler varían de acuerdo con el protocolo.

#### 3.1 Función del encabezado

El encabezado de trama contiene la información de control especificada por el protocolo de capa de enlace de datos para la topología lógica específica y los medios utilizados.

La información de control de trama es única para cada tipo de protocolo.

Los campos típicos del encabezado de trama incluyen:

1. Campo inicio de trama: indica el comienzo de la trama
2. Campos de dirección de origen y destino: indica los nodos de origen y destino en los medios

3. Prioridad/Calidad del Campo de servicio: indica un tipo particular de servicio de comunicación para el procesamiento
4. Campo tipo/longitud: indica el servicio de la capa superior contenida en la trama
5. Campo de control de conexión lógica: utilizada para establecer la conexión lógica entre nodos
6. Campo de control de enlace físico: utilizado para establecer el enlace a los medios
7. Campo de control de flujo: utilizado para iniciar y detener el tráfico a través de los medios
8. Campo de control de congestión: indica la congestión en los medios

### **3.2 Formateo de datos para la transmisión**

#### **3.3 Direccionamiento: hacía donde se dirige la trama**

La capa de enlace de datos proporciona direccionamiento que es utilizado para transportar la trama a través de los medios locales compartidos.

Las direcciones de dispositivo en esta capa se llaman direcciones físicas óMAC.

El direccionamiento de la capa de enlace de datos está contenido en el encabezado de la trama y especifica el nodo de destino de la trama en la red local.

El encabezado de la trama también puede contener la dirección de origen de la trama.

A diferencia de las direcciones lógicas de la Capa 3, que son jerárquicas, las direcciones físicas no indican en qué red está ubicado el dispositivo.

Si el dispositivo es transportado a otra red o subred, funcionará con la misma dirección física de la Capa 2.

Cuando una trama alcanza cada nodo en la topología, el nodo examina la dirección de destino en el encabezado para determinar si es el destino de la trama.

#### **3.4 Función de trailer**

Los protocolos de la capa de enlace de datos agregan un tráiler en el extremo de cada trama.

El tráiler se utiliza para determinar si la trama llegó sin errores. Este proceso se denomina detección de errores.

Observe que es diferente de la corrección de errores.

La detección de errores se logra colocando un resumen lógico o matemático de los bits que comprenden la trama en el tráiler.

##### **3.4.1 Secuencia de verificación de trama**

El campo secuencia de verificación de trama (FCS) se utiliza para determinar si ocurrieron errores de transmisión y recepción de la trama.

La detección de errores se agrega a la capa de enlace de datos porque es ahí donde se transfieren los datos a través de los medios. Los medios son un entorno potencialmente inseguro para los datos.

Las señales en los medios pueden estar sujetas a interferencia, distorsión o pérdida que podría cambiar sustancialmente los valores de los bits que dichas señales representan.

El mecanismo de detección de errores provisto por el uso del campo FCS descubre la mayoría de los errores causados en los medios.

Para asegurarse de que el contenido de la trama recibida en el destino combine con la trama que salió del nodo origen, un nodo de transmisión crea un resumen lógico del contenido de la trama. A esto se lo conoce como valor de comprobación de redundancia cíclica (CRC).

Este valor se coloca en el campo secuencia de verificación de la trama (FCS) para representar el contenido de la trama.

### **3.4.1 Secuencia de verificación de trama**

Cuando la trama llega al nodo de destino, el nodo receptor calcula su propio resumen lógico, o CRC, de la trama.

El nodo receptor compara los dos valores CRC.

Si los dos valores son iguales, se considera que la trama llegó como se transmitió.

Si el valor CRC en el FCS difiere del CRC calculado en el nodo receptor, la trama se descarta.

## **4. Conexión de servicios de capa superior a los medios**

La capa de enlace de datos existe como una capa de conexión entre los procesos de software de las capas por encima de ella y la capa física debajo de ella.

Como tal, prepara los paquetes de capa de red para la transmisión a través de alguna forma de medio, ya sea cobre, fibra o entornos o medios inalámbricos.

En muchos casos, la Capa de enlace de datos está incorporada en una entidad física como tarjeta de interfaz de red (NIC) de Ethernet, que se inserta dentro del bus del sistema de una computadora y hace la conexión entre los procesos de software que se ejecutan en la computadora y los medios físicos.

Sin embargo, la NIC no es solamente una entidad física. El software asociado con la NIC permite que la NIC realice sus funciones de intermediaria preparando los datos para la transmisión y codificando los datos como señales que deben enviarse sobre los medios asociados

## 5. Subcapas de enlace de datos

La capa de enlace de datos a menudo se divide en dos subcapas: una subcapa superior y una subcapa inferior.

La subcapa superior define los procesos de software que proveen servicios a los protocolos de capa de red.

La subcapa inferior define los procesos de acceso a los medios realizados por el hardware.

Las dos subcapas comunes de LAN son:

Control de enlace lógico (LLC) : coloca información en la trama que identifica qué protocolo de capa de red está siendo utilizado por la trama. Esta información permite que varios protocolos de la Capa 3, tales como IP e IPX, utilicen la misma interfaz de red y los mismos medios.

Control de acceso al medio (MAC): proporciona a la capa de enlace de datos el direccionamiento y la delimitación de datos de acuerdo con los requisitos de señalización física del medio y al tipo de protocolo de capa de enlace de datos en uso.

## 6. Estándares

A diferencia de los protocolos de las capas superiores del conjunto TCP/IP, los protocolos de capa de enlace de datos generalmente no están definidos por solicitudes de comentarios (RFC).

A pesar de que el Grupo de trabajo de ingeniería de Internet (IETF) mantiene los protocolos y servicios funcionales para la suite de protocolos TCP/IP en las capas superiores, la IETF no define las funciones ni la operación de esa capa de acceso a la red del modelo.

La capa de acceso de red TCP/IP es el equivalente de las capas de enlace de datos OSI y la física.

Las organizaciones de ingeniería que definen estándares y protocolos abiertos que se aplican a la capa de enlace de datos incluyen:

Organización Internacional para la Estandarización (ISO)

Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)

Instituto Nacional Estadounidense de Estándares (ANSI)

Unión Internacional de Telecomunicaciones (ITU)

A diferencia de los protocolos de la capa superior que están implementados principalmente en el software como el sistema operativo de host o aplicaciones específicas, los procesos de la Capa de enlace de datos se producen tanto en el software como en el hardware.

Los protocolos en esta capa se implementan dentro de la electrónica de los adaptadores de red con los que el dispositivo se conecta a la red física.

Por ejemplo: un dispositivo que implementa la capa de enlace de datos en una computadora sería la tarjeta de interfaz de red (NIC). En una computadora portátil, se utiliza comúnmente un adaptador PCMCIA inalámbrico. Cada uno de estos adaptadores es el hardware que cumple con los estándares y protocolos de la Capa 2.

## 7. Control de acceso al medio

La regulación de la colocación de tramas de datos en los medios es conocida como control de acceso al medio.

El control de acceso al medio es el equivalente a las reglas de tráfico que regulan la entrada de vehículos a una autopista. La ausencia de un control de acceso al medio sería el equivalente a vehículos ignorando el resto del tráfico e ingresando al camino sin tener en cuenta a los otros vehículos.

Sin embargo, no todos los caminos y entradas son iguales. El tráfico puede ingresar a un camino confluyendo, esperando su turno en una señal de parada o respetando el semáforo. Un conductor sigue un conjunto de reglas diferente para cada tipo de entrada.

De la misma manera, hay diferentes formas de regular la colocación de tramas en los medios.

Los protocolos en la capa de enlace de datos definen las reglas de acceso a los diferentes medios.

El método de control de acceso al medio utilizado depende de:

Compartir medios: si y cómo los nodos comparten los medios.

Topología: cómo la conexión entre los nodos se muestra a la capa de enlace de datos.

### 7.1 Control de acceso al medio para medios compartidos

Algunas topologías de red comparten un medio común con varios nodos.

En cualquier momento puede haber una cantidad de dispositivos que intentan enviar y recibir datos utilizando los medios de red.

Hay reglas que rigen cómo esos dispositivos comparten los medios.

Hay dos métodos básicos de control de acceso al medio para medios compartidos:

**Controlado:** Cada nodo tiene su propio tiempo para utilizar el medio

**Basado en la contención:** Todos los nodos compiten por el uso del medio

### **7.1.1 Acceso controlado para medios compartidos**

Al utilizar el método de acceso controlado, los dispositivos de red toman turnos, en secuencia, para acceder al medio.

Si un dispositivo no necesita acceder al medio, la oportunidad de utilizar el medio pasa al siguiente dispositivo en línea. Cuando un dispositivo coloca una trama en los medios, ningún otro dispositivo puede hacerlo hasta que la trama haya llegado al destino y haya sido procesada por el destino.

Aunque el acceso controlado está bien ordenado y provee rendimiento predecible, este método pueden ser ineficientes porque un dispositivo tiene que esperar su turno antes de poder utilizar el medio.

### **7.1.2 Acceso por contención para medios compartidos**

Estos métodos por contención permiten que cualquier dispositivo intent acceder al medio siempre que haya datos para enviar.

Para evitar caos completo en los medios, estos métodos usan un proceso de Acceso múltiple por detección de portadora (CSMA) para detectar primero si los medios están transportando una señal.

Si se detecta una señal portadora en el medio desde otro nodo, quiere decir que otro dispositivo está transmitiendo.

Cuando un dispositivo está intentando transmitir y nota que el medio está ocupado, esperará e intentará después de un período de tiempo corto.

Si no se detecta una señal portadora, el dispositivo transmite sus datos.

Las redes Ethernet e inalámbricas utilizan control de acceso al medio por contención.

Es posible que el proceso CSMA falle si dos dispositivos transmiten al mismo tiempo. A esto se lo denomina colisión de datos.

Si esto ocurre, los datos enviados por ambos dispositivos se dañarán y deberán enviarse nuevamente.

Los métodos de control de acceso al medio por contención no tienen la sobrecarga de los métodos de acceso controlado. No se requiere un mecanismo para analizar quién posee el turno para acceder al medio.

Sin embargo, los sistemas por contención no escalan bien bajo un uso intensivo de los medios. A medida que el uso y el número de nodos aumenta, la probabilidad de acceder a los medios con éxito sin una colisión disminuye.

CSMA es generalmente implementado junto con un método para resolver la contención del medio.

Los dos métodos comúnmente utilizados son:  
CSMA/Detección de colisión (CSMA/CD)



## CSMA/Prevención de colisiones (CSMA/CA)

### 7.1.2.1 CSMA/CD

Todos los dispositivos de red que tienen mensajes para enviar deben escuchar antes de transmitir.

Si un dispositivo detecta una señal de otro dispositivo, esperará durante un período especificado antes de intentar transmitir.

Cuando no se detecte tráfico, un dispositivo transmitirá su mensaje.

Mientras se lleva a cabo la transmisión, el dispositivo continúa escuchando para detectar tráfico o colisiones en la LAN.

Las formas tradicionales de Ethernet usan este método.

### 7.1.2.2 CSMA/CA

En CSMA/Prevención de colisiones, el dispositivo examina los medios para detectar la presencia de una señal de datos.

Si el medio está libre, el dispositivo envía una notificación a través del medio, sobre su intención de utilizarlo.

El dispositivo luego envía los datos.

Este método es utilizado por las tecnologías de redes inalámbricas 802.11.

## 8. Control de acceso al medio para medios no compartidos

Los protocolos de control de acceso al medio para medios no compartidos requieren poco o ningún control antes de colocar tramas en los medios. Estos protocolos tienen reglas y procedimientos más simples para el control de acceso al medio. Tal es el caso de las topologías punto a punto.

En las topologías punto a punto, los medios interconectan sólo dos nodos. En esta configuración, los nodos no necesitan compartir los medios con otros hosts ni determinar si una trama está destinada para ese nodo.

Por lo tanto, los protocolos de capa de enlace de datos hacen poco para controlar el acceso a medios no compartidos.

### 8.1 Full Duplex y Half Duplex

En conexiones punto a punto, la Capa de enlace de datos tiene que considerar si la comunicación es half-duplex o fullduplex.

Comunicación half-duplex quiere decir que los dispositivos pueden transmitir y recibir en los medios pero no pueden hacerlo simultáneamente. Ethernet ha establecido reglas de arbitraje para resolver conflictos que surgen de instancias donde más de una estación intenta transmitir al mismo tiempo.

En la comunicación full-duplex, los dos dispositivos pueden transmitir y recibir en los medios al mismo tiempo. La capa de enlace de datos supone que los medios están disponibles para transmitir para ambos nodos en cualquier momento. Por lo tanto, no hay necesidad de arbitraje de medios en la capa de enlace de datos.

## **9. Comparación entre la topología lógica y la topología física**

La topología de una red es la configuración o relación de los dispositivos de red y las interconexiones entre ellos.

La topología física es una configuración de nodos y las conexiones físicas entre ellos. La representación de cómo se usan los medios para interconectar los dispositivos es la topología física.

Una topología lógica es la forma en que una red transfiere tramas de un nodo al siguiente. Esta configuración consiste en conexiones virtuales entre los nodos de una red independiente de su distribución física. Está estrechamente relacionada con el mecanismo utilizado para administrar el acceso a la red.

La topología física o cableada de una red probablemente no sea la misma que la topología lógica.

Las topologías lógicas generalmente utilizadas en redes son:

Punto a Punto

Multi-Acceso

Anillo

### **9.1 Topología punto a punto**

Una topología punto a punto conecta dos nodos directamente entre sí.

En redes de datos con topologías punto a punto, el protocolo de control de acceso al medio puede ser muy simple. Todas las tramas en los medios sólo pueden viajar a los dos nodos o desde éstos. El nodo en un extremo coloca las tramas en los medios y el nodo en el otro extremo las saca de los medios del circuito punto a punto.

En redes punto a punto, si los datos sólo pueden fluir en una dirección a la vez, está operando como un enlace half-duplex. Si los datos pueden fluir con éxito a través del enlace desde cada nodo simultáneamente, es un enlace duplex.

#### **9.1.1 Redes punto a punto lógicas**

Los nodos de los extremos que se comunican en una red punto a punto pueden estar conectados físicamente a través de una cantidad de dispositivos intermedios.

Sin embargo, el uso de dispositivos físicos en la red no afecta la topología lógica.

Como se muestra en la figura, los nodos de origen y destino pueden estar conectados indirectamente entre sí a través de una distancia geográfica.

La conexión lógica de punto a punto entre dos nodos puede no ser necesariamente entre dos nodos físicos en cada extremo de un enlace físico único.

## 9.2 Topología multiacceso

Una topología lógica multiacceso permite a una cantidad de nodos comunicarse utilizando los mismos medios compartidos.

Los datos desde un sólo nodo pueden colocarse en el medio en cualquier momento. Todos los nodos ven todas las tramas que están en el medio, pero sólo el nodo al cual la trama está direccionada procesa los contenidos de la trama.

Hacer que varios nodos compartan el acceso a un medio requiere un método de control de acceso al medio de enlace de datos que regule la transmisión de datos y, por lo tanto, reduzca las colisiones entre las diferentes señales.

Los métodos de control de acceso al medio utilizado por las topologías multiacceso son generalmente CSMA/CD o CSMA/CA. Ver animación 7.2.6

## 9.3 Topología en anillo

En una topología lógica de anillo, cada nodo recibe una trama por turno. Si la trama no está direccionada al nodo, el nodo pasa la trama al nodo siguiente. Esto permite que un anillo utilice una técnica de control de acceso al medio llamada paso de tokens.

Los nodos en una topología lógica de anillo retiran la trama del anillo, examinan la dirección y la envían si no está dirigida para ese nodo. En un anillo, todos los nodos alrededor del anillo entre el nodo de origen y de destino examinan la trama.

Existen múltiples técnicas de control de acceso a los medios que podrían usarse con un anillo lógico, dependiendo del nivel de control requerido. Por ejemplo: sólo una trama a la vez es generalmente transportada por el medio. Si no se están transmitiendo datos, se colocará una señal (conocida como token) en el medio y un nodo sólo puede colocar una trama de datos en el medio cuando tiene el token.

Recuerde que la capa de enlace de datos "ve" una topología lógica de anillo. La topología del cableado físico real puede ser otra topología.

## 10. Protocolos de la capa de enlace de datos

El protocolo de la Capa 2 utilizado depende de la topología lógica de la red y de la implementación de la capa física.

Debido al amplio rango de medios físicos utilizados a través de un rango de topologías en interconexión de redes, hay una gran cantidad de protocolos de la Capa 2 en uso.

Los protocolos principales de capa 2 son:

- Ethernet
- Protocolo Punto a Punto (PPP)
- Control de enlace de datos de alto nivel (HDLC)
- Frame Relay
- Modo de transferencia asincrónico (ATM)

### 10.1 Protocolo Ethernet para LAN

Ethernet es una familia de tecnologías de interconexión de redes que se define en los estándares 802.2 y 802.3.

Los estándares de Ethernet definen los protocolos de la Capa 2 y las tecnologías de la Capa 1.

Ethernet es la tecnología LAN más ampliamente utilizada y soporta anchos de banda de datos de 10, 100, 1000, o 10 000 Mbps.

Ethernet utiliza CSMA/CD como métodos de acceso al medio.

El medio compartido requiere que el encabezado del paquete de Ethernet utilice la dirección de la capa de enlace de datos para identificar los nodos de origen y destino.

Como con la mayoría de los protocolos LAN, esta dirección se llama dirección MAC del nodo.

Una dirección MAC de Ethernet es de 48 bits y generalmente se representa en formato hexadecimal.

### 10.1 Protocolo Ethernet para LAN (II)

La trama de Ethernet tiene muchos campos y es casi idéntica para todas las velocidades de Ethernet.

Sin embargo, en la capa física, las diferentes versiones de Ethernet colocan los bits sobre el medio de forma diferente.

### 10.2 Protocolo punto a punto para WAN

El protocolo punto a punto (PPP) es un protocolo utilizado para entregar tramas entre dos nodos.

A diferencia de muchos protocolos de capa de enlace de datos, definidos por las organizaciones de ingeniería eléctrica, el estándar PPP está definida por RFC.

PPP se puede utilizar en diversos medios físicos, lo que incluye cable de par trenzado, líneas de fibra óptica o transmisión satelital.

### **10.3 Protocolo inalámbrico para LAN**

802.11 es una extensión de los estándares IEEE 802.

El estándar IEEE 802.11, comúnmente llamada Wi-Fi, es un sistema por contención que utiliza un proceso de acceso al medio de Acceso múltiple con detección de portadora y prevención de colisiones (CSMA/CA).

Las redes 802.11 también usan Acuse de recibo de enlace de datos para confirmar que una trama se recibió con éxito.

Si la estación transmisora no detecta la trama de reconocimiento, ya sea porque la trama de datos original o el reconocimiento no se recibieron intactos, se retransmite la trama.

## **11. Ethernet**

En 1985, el comité de estándares para Redes Metropolitanas y Locales del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) publicó los estándares para las LAN. Estos estándares comienzan con el número 802.

Ethernet opera en las dos capas inferiores del modelo OSI: la capa de enlace de datos y la capa física.

La Capa 1 de Ethernet tiene un papel clave en la comunicación que se produce entre los dispositivos, pero tiene limitaciones.

Ethernet en la Capa 2 se ocupa de estas limitaciones.

### **11.1 Control del enlace lógico**

Ethernet separa las funciones de la capa de Enlace de datos en dos subcapas diferenciadas: la subcapa Control de enlace lógico (LLC) y la subcapa Control de acceso al medio (MAC).

Para Ethernet, el estándar IEEE 802.2 describe las funciones de la subcapa LLC y el estándar 802.3 describe las funciones de la subcapa MAC y de la capa física.

El Control de enlace lógico se encarga de la comunicación entre las capas superiores y el software de red, y las capas inferiores, que generalmente es el hardware.

La subcapa LLC toma los datos del protocolo de la red, que generalmente son un paquete IPv4, y agrega información de control para ayudar a entregar el paquete al nodo de destino.

En una computadora, el LLC puede considerarse como el controlador de la Tarjeta de interfaz de red (NIC).

El controlador de la NIC (Tarjeta de interfaz de red) es un programa que interactúa directamente con el hardware en la NIC para pasar los datos entre los medios y la subcapa de Control de Acceso al medio (MAC).

## **11.2 MAC: envío de datos a los medios**

El Control de acceso al medio (MAC) es la subcapa de Ethernet inferior de la capa de Enlace de datos.

El hardware implementa el Control de acceso al medio, generalmente en la Tarjeta de interfaz de red (NIC).

La subcapa MAC de Ethernet tiene dos responsabilidades principales:

- A. Encapsulación de datos
- B. Control de Acceso al medio

### 11.2.1 Encapsulación de datos

La encapsulación de datos proporciona tres funciones principales:

- Delimitación de trama
- Direccionamiento
- Detección de errores

El proceso de encapsulación de datos incluye el armado de la trama antes de la transmisión y el análisis de la trama al momento de recibir una trama.

Cuando forma una trama, la capa MAC agrega un encabezado y un tráiler a la PDU de Capa 3.

El proceso de encapsulación también posibilita el direccionamiento de la capa de Enlace de datos.

Cada encabezado Ethernet agregado a la trama contiene la dirección física (dirección MAC) que permite que la trama se envíe a un nodo de destino.

Una función adicional de la encapsulación de datos es la detección de errores.

Cada trama de Ethernet contiene un tráiler con una comprobación cíclica de redundancia (CRC) de los contenidos de la trama.

Una vez que se recibe una trama, el nodo receptor crea una CRC para compararla con la de la trama.

Si estos dos cálculos de CRC coinciden, puede asumirse que la trama se recibió sin errores.

## 11.2.2 Control de acceso al medio

La subcapa MAC controla la colocación de tramas en los medios y el retiro de tramas de los medios.

Como su nombre lo indica, se encarga de administrar el control de acceso al medio.

La topología lógica subyacente de Ethernet es un bus de multiacceso.

Esto significa que todos los nodos (dispositivos) en ese segmento de la red comparten el medio. Esto significa además que todos los nodos de ese segmento reciben todas las tramas transmitidas por cualquier nodo de dicho segmento.

Debido a que todos los nodos reciben todas las tramas, cada nodo debe determinar si debe aceptar y procesar una determinada trama.

Esto requiere analizar el direccionamiento en la trama provisto por la direcciónMAC.

Ethernet ofrece un método para determinar cómo comparten los nodos el acceso al medio.

El método de control de acceso a los medios para Ethernet clásica es el Acceso múltiple con detección de portadora con detección de colisiones (CSMA/CD).

## 11.3 Primeros medios Ethernet

Leer apuntes

## 11.4 La trama Ethernet

La estructura de la trama de Ethernet agrega encabezados y tráilers a la PDU de Capa 3 para encapsular el mensaje que se envía.

Tanto el encabezado como el tráiler de Ethernet tienen varias secciones de información que el protocolo Ethernet utiliza.

Cada sección de la trama se denomina campo.

Hay dos estilos de tramas de Ethernet: el IEEE 802.3 (original) y el IEEE 802.3 revisado.

Las diferencias entre los estilos de tramas son mínimas. La diferencia más significativa entre el IEEE 802.3 (original) y el IEEE 802.3 revisado es el agregado de un delimitador de inicio de trama (SFD) y un pequeño cambio en el campo Tipo que incluye la Longitud.

### 11.4.1 Campos de la trama

Los campos Preámbulo (7 bytes) y Delimitador de inicio de trama (SFD) (1 byte) se utilizan para la sincronización entre los dispositivos de envío y de recepción. Estos ocho primeros bytes de la trama se utilizan para captar la atención de los nodos receptores. Básicamente, los primeros bytes le indican al receptor que se prepare para recibir una trama nueva.

Campo Dirección MAC de destino (6 bytes): es el identificador del receptor deseado. Como recordará, la Capa 2 utiliza esta dirección para ayudar a los dispositivos a determinar si la trama viene dirigida a ellos. La dirección de la trama se compara con la dirección MAC del dispositivo. Si coinciden, el dispositivo acepta la trama.

Campo Dirección MAC de origen (6 bytes): identifica la NIC o interfaz que origina la trama.

Campo Tipo (2 bytes): define la longitud exacta del campo Datos de la trama. En este campo debe ingresarse una longitud o un tipo. Sin embargo, sólo uno u otro podrá utilizarse en una determinada implementación. Si el objetivo del campo es designar un tipo, el campo Tipo describe qué protocolo se implementa.

Campos Datos (de 46 a 1500 bytes): contienen los datos encapsulados de una capa superior, que es un paquete IPv4. Todas las tramas deben tener al menos 64 bytes de longitud. Si se encapsula un paquete pequeño, se introduce un relleno que se utiliza para aumentar el tamaño de la trama hasta alcanzar este tamaño mínimo.

El campo Secuencia de verificación de trama (FCS) (4 bytes) se utiliza para detectar errores en la trama. Utiliza una comprobación cíclica de redundancia (CRC). El dispositivo emisor incluye los resultados de una CRC en el campo FCS de la trama.

El dispositivo receptor recibe la trama y genera una CRC para detectar errores. Si los cálculos coinciden, significa que no se produjo ningún error. Los cálculos que no coinciden indican que los datos cambiaron y, por consiguiente, se descarta la trama. Un cambio en los datos podría ser resultado de una interrupción de las señales eléctricas que representan los bits.

#### **11.4.2 Tamaño de la trama Ethernet**

El estándar Ethernet original definió el tamaño mínimo de trama en 64 bytes y el tamaño máximo de trama en 1518 bytes.

Esto incluye todos los bytes del campo Dirección MAC de destino a través del campo Secuencia de verificación de trama (FCS).

Los campos Preámbulo no se incluye en la descripción del tamaño de una trama.

El estándar IEEE 802.3ac, publicado en 1998, amplió el tamaño de trama máximo permitido a 1522 bytes.

Si el tamaño de una trama transmitida es menor que el mínimo o mayor que el máximo, el dispositivo receptor descarta la trama.

#### **11.4.3 Dirección MAC de Ethernet**

El problema más importante que debía resolverse era cómo identificar cada uno de los dispositivos.



La señal podía enviarse a todos los dispositivos, pero ¿cómo podía determinar cada uno de los dispositivos si era el receptor del mensaje? Se creó un identificador único, denominado dirección de Control de acceso al medio (MAC), para ayudar a determinar las direcciones de origen y destino dentro de una red Ethernet.

La dirección MAC se agrega como parte de una PDU de Capa 2.

Una dirección MAC de Ethernet es un valor binario de 48 bits expresado como 12 dígitos hexadecimales.

#### **11.4.1 Estructura de la dirección MAC**

El valor de la dirección MAC es el resultado directo de las normas implementadas por el IEEE para proveedores con el objetivo de garantizar direcciones únicas para cada dispositivo Ethernet.

Las normas establecidas por el IEEE obligan a los proveedores de dispositivos Ethernet a registrarse en el IEEE.

El IEEE le asigna a cada proveedor un código de 3 bytes, denominado Identificador único organizacional (OUI). El IEEE obliga a los proveedores a respetar dos normas simples:

Todas las direcciones MAC asignadas a una NIC u otro dispositivo Ethernet deben utilizar el OUI que se le asignó a dicho proveedor como los 3 primeros bytes.

Se les debe asignar un valor exclusivo a todas las direcciones MAC con el mismo OUI (Identificador exclusivo de organización) (código del fabricante o número de serie) en los últimos 3 bytes.

Todos los dispositivos conectados a una LAN Ethernet tienen interfaces con direcciones MAC.

Diferentes fabricantes de hardware y software pueden representar las direcciones MAC en distintos formatos hexadecimales. Los formatos de las direcciones pueden ser similares a 00-05-9A-3C-78-00, 00:05:9A:3C:78:00 ó 0005.9A3C.7800.

Las direcciones MAC se asignan a estaciones de trabajo, servidores, impresoras, switches y routers.

La dirección MAC se suele denominar dirección grabada (BIA) porque se encuentra grabada en la ROM (Memoria de sólo lectura) de la NIC. Esto significa que la dirección se codifica en el chip de la ROM de manera permanente (el software no puede cambiarla).

Sin embargo, cuando se inicia el equipo la NIC copia la dirección a la RAM (Memoria de acceso aleatorio).

Cuando se examinan tramas se utiliza la dirección que se encuentra en la RAM como dirección de origen para compararla con la dirección de destino.

#### **11.4.2 Visualización de la MAC**

Una herramienta útil para analizar la dirección MAC de nuestra computadora es ipconfig / all o ifconfig.

## **12. Ethernet unicast, multicast y broadcast**

En Ethernet se utilizan distintas direcciones MAC para la capa 2: comunicaciones unicast, multicast y broadcast.

Una dirección MAC unicast es la dirección exclusiva que se utiliza cuando se envía una trama desde un dispositivo de transmisión único hacia un dispositivo de destino único.

Con broadcast, el paquete contiene una dirección IP de destino con todos unos (1) en la porción de host. Esta numeración en la dirección significa que todos los hosts de esa red local (dominio de broadcast) recibirán y procesarán el paquete. Una dirección IP de broadcast para una red necesita una dirección MAC de broadcast correspondiente en la trama de Ethernet. En redes Ethernet, la dirección MAC de broadcast contiene 48 unos que se muestran como el hexadecimal FF-FF-FF-FF-FF-FF.

Las direcciones multicast le permiten a un dispositivo de origen enviar un paquete a un grupo de dispositivos.

Una dirección IP de grupo multicast se asigna a los dispositivos que pertenecen a un grupo multicast. El intervalo de direcciones multicast es de 224.0.0.0 a 239.255.255.255. Debido a que las direcciones multicast representan un grupo de direcciones (a veces denominado un grupo de hosts), sólo pueden utilizarse como el destino de un paquete.

El origen siempre tendrá una dirección unicast.

Ejemplos de dónde se utilizarían las direcciones multicast serían el juego remoto, en el que varios jugadores se conectan de manera remota pero juegan el mismo juego, y el aprendizaje a distancia a través de videoconferencia, en el que varios estudiantes se conectan a la misma clase.

## **12. Ethernet unicast, multicast y broadcast**

La dirección IP multicast requiere una dirección MAC multicast correspondiente para poder enviar tramas en una red local. La dirección MAC multicast es un valor especial que comienza con 01-00-5E en hexadecimal. El valor termina con la conversión de los 23 bits inferiores de la dirección IP del grupo multicast en los 6 caracteres hexadecimales restantes de la dirección de Ethernet. El bit restante en la dirección MAC es siempre "0".

## **13. Hub**

Un concentrador o hub es un dispositivo que permite centralizar el cableado de una red y poder ampliarla.

Los hubs concentran las conexiones, es decir, toman un grupo de nodos y permiten que la red los trate como una sola unidad.

Cuando una trama llega a un puerto, se lo copia a los demás puertos para que todos los segmentos de la LAN reciban la trama.

Pueden producirse colisiones entre los dispositivos que conectan y dentro de los mismos hubs.

Además, la utilización de hubs para proporcionar acceso a la red a una mayor cantidad de usuarios reduce el rendimiento para cada usuario, ya que debe compartirse la capacidad fija de los medios entre cada vez más dispositivos.

Los dispositivos conectados que tienen acceso a medios comunes a través de un hub o una serie de hubs conectados directamente conforman lo que se denomina dominio de colisiones.

Un dominio de colisiones también se denomina segmento de red.

Se define dominio de colisión como un grupo de dispositivos conectados al mismo medio físico, de tal manera que si dos dispositivos acceden al medio al mismo tiempo, el resultado sea una colisión entre las dos señales.

### **13.1 Ethernet antigua**

La Ethernet clásica utiliza hubs para interconectar los nodos del segmento de LAN.

El hub reenvía todos los bits a todos los dispositivos conectados al hub.

Esto obliga a todos los dispositivos de la LAN a compartir el ancho de banda de los medios.

Además, esta implementación de Ethernet clásica origina a menudo grandes niveles de colisiones en la LAN.

Debido a estos problemas de rendimiento, este tipo de LAN Ethernet tiene un uso limitado en las redes actuales. Las implementaciones de Ethernet con hubs se utilizan generalmente en la actualidad en LAN pequeñas o LAN con pocos requisitos de ancho de banda.

Los switches brindan una alternativa para solucionar los problemas de la Ethernet clásica.

## **14. Switch**

Un conmutador o switch es un dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI.

Su función es interconectar dos o más segmentos de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Los switches permiten la segmentación de la LAN en distintos dominios de colisiones.

Cada puerto de un switch representa un dominio de colisiones distinto y brinda un ancho de banda completo al nodo conectado a dicho puerto.

Con una menor cantidad de nodos en cada dominio de colisiones, se produce un aumento en el ancho de banda promedio disponible para cada nodo y se reducen las colisiones.

## 14.1 Ancho de banda dedicado

Cada nodo dispone del ancho de banda de los medios completo en la conexión entre el nodo y el switch.

Debido a que un hub replica las señales que recibe y las envía a todos los demás puertos, los hubs de Ethernet deben compartir el mismo ancho de banda para este bus.

Con los switches, cada dispositivo tiene una conexión punto a punto dedicada entre el dispositivo y el switch.

Pueden compararse dos LAN de 100 Mbps, cada una de ellas con 10 nodos. En el segmento de red A, los 10 nodos se conectan a un hub. Cada nodo comparte el ancho de banda de 100 Mbps disponible.

Esto ofrece un promedio de 10 Mbps para cada nodo. En el segmento de red B, los 10 nodos se conectan a un switch. En este segmento, los 10 nodos tienen el ancho de banda completo de 100 Mbps disponible.

## 14.2 Funcionamiento del switch

Para lograr su fin, los switches LAN Ethernet realizan cinco operaciones básicas:

Aprendizaje

Actualización

Inundación (flooding)

Reenvío selectivo

Filtrado

### 14.2.1 Aprendizaje

La tabla MAC debe llenarse con las direcciones MAC y sus puertos correspondientes.

El proceso de aprendizaje permite que estos mapeos se adquieran dinámicamente durante el funcionamiento normal.

A medida que cada trama ingresa al switch, el switch analiza la dirección MAC de origen. Mediante un proceso de búsqueda, el switch determina si la tabla ya contiene una entrada para esa dirección MAC.

Si no existe ninguna entrada, el switch crea una nueva entrada en la tabla MAC utilizando la dirección MAC de origen y asocia la dirección con el puerto en el que llegó la entrada.

Ahora, el switch puede utilizar este mapeo para reenviar tramas a este nodo.

### 14.2.2 Actualización

Las entradas de la tabla MAC que se adquirieron mediante el proceso de Aprendizaje reciben una marca horaria.

La marca horaria se utiliza como instrumento para eliminar las entradas antiguas de la tablaMAC.

Después de que se crea una entrada en la tabla MAC, un proceso comienza una cuenta regresiva utilizando la marca horaria como el valor inicial.

Una vez que el valor alcanza 0, la entrada de la tabla se actualizará la próxima vez que el switch reciba una trama de ese nodo en el mismo puerto.

### **14.2.3 Inundación**

Si el switch no sabe a qué puerto enviar una trama porque la dirección MAC de destino no se encuentra en la tabla MAC, el switch envía la trama a todos los puertos, excepto al puerto en el que llegó la trama.

El proceso que consiste en enviar una trama a todos los segmentos se denomina inundación.

La inundación también se utiliza para tramas que se envían a la dirección MAC de broadcast.

### **14.2.4 Reenvío selectivo**

El reenvío selectivo es el proceso por el cual se analiza la dirección MAC de destino de una trama y se la reenvía al puerto correspondiente. Ésta es la función principal del switch. Cuando una trama de un nodo llega al switch y el switch ya aprendió su dirección MAC, dicha dirección se hace coincidir con una entrada de la tabla MAC y la trama se reenvía al puerto correspondiente.

En lugar de saturar la trama hacia todos los puertos, el switch envía la trama al nodo de destino a través del puerto indicado.

Esta acción se denomina reenvío.

### **14.2.5 Filtrado**

En algunos casos, la trama no se reenvía. Este proceso se denomina filtrado de la trama.

Uno de los usos del filtrado ya se describió: un switch no reenvía una trama al mismo puerto en el que llega.

El switch también descartará una trama corrupta. Si una trama no aprueba la verificación CRC, dicha trama se descarta.

Otra razón por la que una trama se filtra es por motivos de seguridad. Un switch tiene configuraciones de seguridad para bloquear tramas hacia o desde direcciones MAC selectivas o puertos específicos.

## **15. El protocolo ARP**

El protocolo ARP (Address Resolution Protocol) ofrece dos funciones básicas:

Resolución de direcciones IPv4 a direcciones MAC

Mantenimiento de una caché de las asignaciones

## **15.1 Resolución de direcciones IPv4 a direcciones MAC**

Para que una trama se coloque en los medios de la LAN, debe contar con una dirección MAC de destino.

Cuando se envía un paquete a la capa de Enlace de datos para que se lo encapsule en una trama, el nodo consulta una tabla en su memoria para encontrar la dirección de la capa de Enlace de datos que se mapea a la dirección IPv4 de destino.

Esta tabla se denomina tabla ARP o caché ARP.

Cada entrada o fila de la tabla ARP tiene un par de valores: una dirección IP y una direcciónMAC.

La relación entre los dos valores se denomina mapa, que simplemente significa que usted puede localizar una dirección IP en la tabla y descubrir la direcciónMAC correspondiente.

## **15.2 Mantenimiento de una tabla ARP**

La tabla ARP se mantiene dinámicamente.

Existen dos maneras en las que un dispositivo puede reunir direcciones MAC.

Una es monitorear el tráfico que se produce en el segmento de la red local. A medida que un nodo recibe tramas de los medios, puede registrar las direcciones IP yMAC de origen comomapeos en la tabla ARP.

Otra manera en la que un dispositivo puede obtener un par de direcciones es emitir una solicitud de ARP. El ARP envía un broadcast de Capa 2 a todos los dispositivos de la LAN Ethernet. La trama contiene un paquete de solicitud de ARP con la dirección IP del host de destino. El nodo que recibe la trama y que identifica la dirección IP como si fuera la suya responde enviando un paquete de respuesta de ARP al emisor como una trama unicast. Esta respuesta se utiliza entonces para crear una entrada nueva en la tabla ARP.

## **15.2 Mantenimiento de una tabla ARP**

Además, pueden ingresarse entradas estáticas de mapas en una tabla ARP, pero esto no sucede con frecuencia.

Las entradas estáticas de la tabla ARP caducan cuando pasa el tiempo y deben eliminarse en forma manual.

## **15.3 El proceso de ARP: destinos fuera de la red local**

Si el host IPv4 de destino no se encuentra en la red local, el nodo de origen necesita enviar la trama a la interfaz del router que es el gateway que se utiliza para llegar a dicho destino.

El nodo de origen utilizará la dirección MAC del gateway como dirección de destino para las tramas que contengan un paquete IPv4 dirigido a hosts que se encuentren en otras redes.

Cuando un host crea un paquete para un destino, compara la dirección IP de destino con su propia dirección IP para determinar si las dos direcciones IP se encuentran en la misma red de Capa 3.

Si el host receptor no se encuentra en la misma red, el origen utiliza el proceso de ARP para determinar una dirección MAC para la interfaz del router que sirve de gateway.

En caso de que la entrada de gateway no se encuentre en la tabla, el proceso de ARP normal enviará una solicitud de ARP para recuperar la dirección MAC asociada con la dirección IP de la interfaz del router.

#### **15.4 Eliminación de mapeos de direcciones**

Para cada dispositivo, un temporizador de caché de ARP elimina las entradas ARP que no se hayan utilizado durante un período de tiempo especificado.

Los tiempos difieren dependiendo del dispositivo y su sistema operativo.

Por ejemplo, algunos sistemas operativos de Windows almacenan las entradas de caché de ARP durante 2 minutos. Si la entrada se utiliza nuevamente durante ese tiempo, el temporizador ARP para esa entrada se extiende a 10 minutos.

También pueden utilizarse comandos para eliminar manualmente todas o algunas de las entradas de la tabla ARP.

Después de eliminar una entrada, el proceso para enviar una solicitud de ARP y recibir una respuesta ARP debe ocurrir nuevamente para ingresar el mapa en la tabla ARP.