

Estandarización



Estándares

- Problemática:
 - Fabricantes y proveedores de redes , cada uno con sus propias ideas de cómo se deben hacer las cosas
 - Sin coordinación = caos total
 - Afectados: usuarios
- Solución:
 - Acordar la adopción de algunos estándares para redes



Estándares

- Beneficios:
 - Permiten que computadoras diferentes se comuniquen
 - Permiten incrementar el mercado de productos que se ajustan al estándar



Estándares

- Categorías
 - De facto (de hecho) surgieron sin ningún plan formal:

- IBM
- UNIX



- De jure (por derecho) son formales, legales, adoptados por alguna institución de estandarización autorizada.

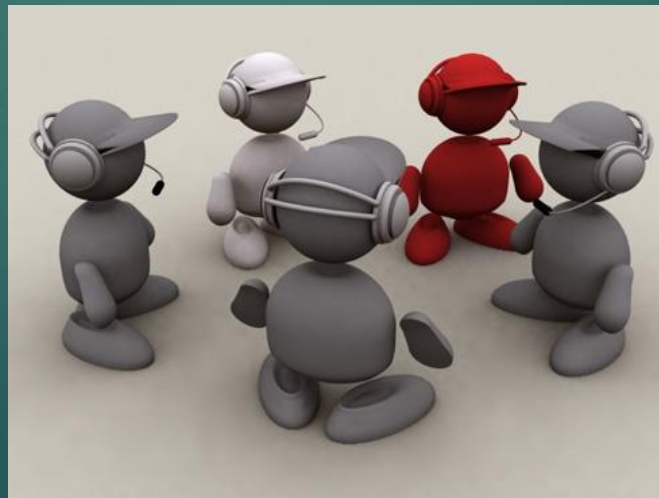


Organismos de estandarización

Organismos

Se dividen en dos clases

- Los establecidos por acuerdos entre los gobiernos de cada país.
- Los incluidos de manera voluntaria, sin acuerdos entre organizaciones.



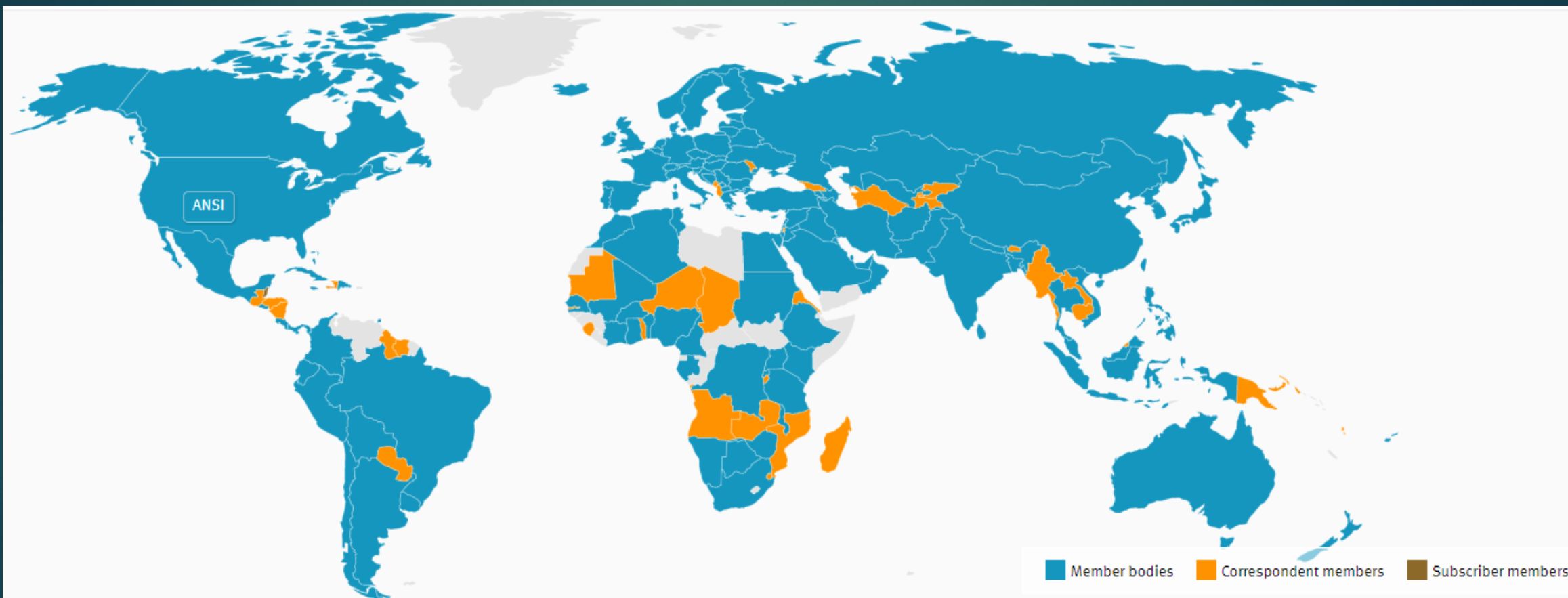
ISO




ISO International Organization for Standardization

Nace después de la Segunda Guerra Mundial (fue creada el 23 de febrero de 1947),

- ▶ Estándares de gestión de calidad.
- ▶ Estándares de gestión ambiental.
- ▶ Estándares de salud y seguridad.
- ▶ Estándares de gestión energética.
- ▶ Normas de seguridad alimentaria.
- ▶ Estándares de seguridad de TI.



This map is designed to visually demonstrate the geographic distribution of our Members. The boundaries shown do not imply an official endorsement or acceptance by ISO.

- 
- ▶ La ISO es una red de los institutos de normas nacionales de 165 países.
 - ▶ Un miembro por país.
 - ▶ Las normas desarrolladas por ISO son voluntarias.
 - ▶ Es un organismo no gubernamental y no depende de ningún otro organismo internacional, por lo tanto, no tiene autoridad para imponer sus normas a ningún país.
 - ▶ <https://www.iso.org/>



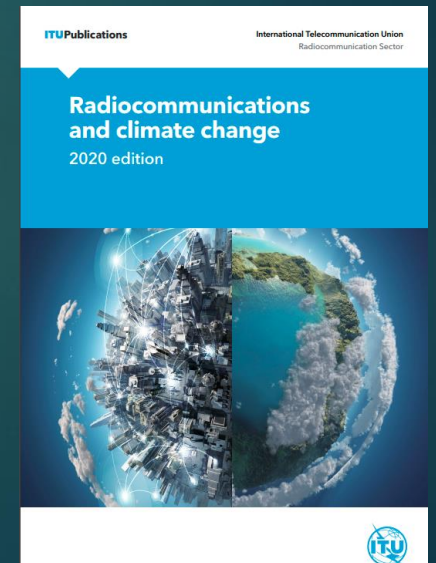
ITU

ITU International Telecommunication Union

- ▶ La UIT es el organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación
- ▶ Antecedentes:
 - ▶ Unión Telegráfica Internacional (UTI y la Unión Radiotelegráfica Internacional (URI).

ITU

- En general, la normativa generada por la ITU está contenida en un amplio conjunto de documentos denominados **Recomendaciones, agrupados por Series**. Cada serie está compuesta por las Recomendaciones correspondientes a un mismo tema.
- <https://www.itu.int/es/Pages/default.aspx>



IEEE

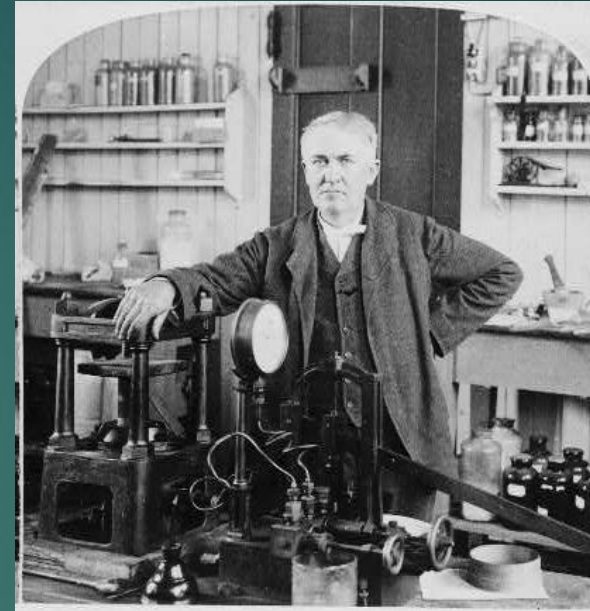




IEEE institute of Electrical and Electronics Engineers

- ▶ Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como:
 - ▶ Ingenieros eléctricos,
 - ▶ Ingenieros en electrónica,
 - ▶ Científicos de la computación,
 - ▶ Ingenieros en informática e
 - ▶ Ingenieros en telecomunicación.

- Su creación se remonta al año 1884
- Fundadores :
 - Thomas Alva Edison,
 - Alexander Graham Bell y
 - Franklin Leonard Pope.
- En 1963 adoptó el nombre de **IEEE**
- Su trabajo es promover la creatividad, el desarrollo y la integración, compartir y aplicar los avances en las tecnologías de la información, electrónica y ciencias en general para beneficio de la humanidad y de los mismos profesionales.
- <https://www.ieee.org/>



ANSI



ANSI American National Standards Institute

- ▶ Es una organización sin ánimo de lucro que supervisa el desarrollo de estándares para **productos, servicios, procesos y sistemas** en los **Estados Unidos**.
- ▶ ANSI es miembro de la Organización Internacional para la Estandarización (ISO) y de la Comisión Electrotécnica Internacional (International Electrotechnical Commission, IEC).
- ▶ La organización también coordina estándares del país estadounidense con estándares internacionales.
- ▶ <https://www.ansi.org/>





NOM

NOM

NOM Norma Oficial Mexicana

- ▶ Son regulaciones técnicas de observancia obligatoria expedidas por las dependencias competentes.
- ▶ Ejemplos:
- ▶ Salud
- ▶ Seguridad Industrial
- ▶ Telecomunicaciones

<https://www.sinec.gob.mx/SINEC/Vista/Normalizacion/BusquedaNormas.xhtml>



EIA

EIA Electronic Industries Alliance

- Fue una organización formada por la **asociación** de las **compañías electrónicas** y de alta tecnología de los **Estados Unidos**
- Junto con TIA, publicó la norma para cableado estructurado, actualmente sus operaciones fueron incluidas por TIA





TIA

TIA Telecommunications Industry Association

TIA está acreditada por el American National Standards Institute (ANSI) como una organización de desarrollo de estándares (SDO). Los comités de ingeniería de TIA crean estándares y documentos técnicos basados en las pautas establecidas por los Requisitos Esenciales de ANSI.

<https://tiaonline.org/>



El BroadBand Forum

Es la organización líder de la industria de las comunicaciones centrada en acelerar la innovación, los estándares y el desarrollo de ecosistemas de banda ancha.

<https://www.broadband-forum.org/>

Modelo OSI

Modelo OSI

- Modelo de referencia para la interconexión de sistemas abiertos.
- Proporciona una descripción generalizada de las herramientas de interconectividad de redes
- Estándar 7498-1
- <https://www.iso.org/standard/20269.html>

Sistema abierto

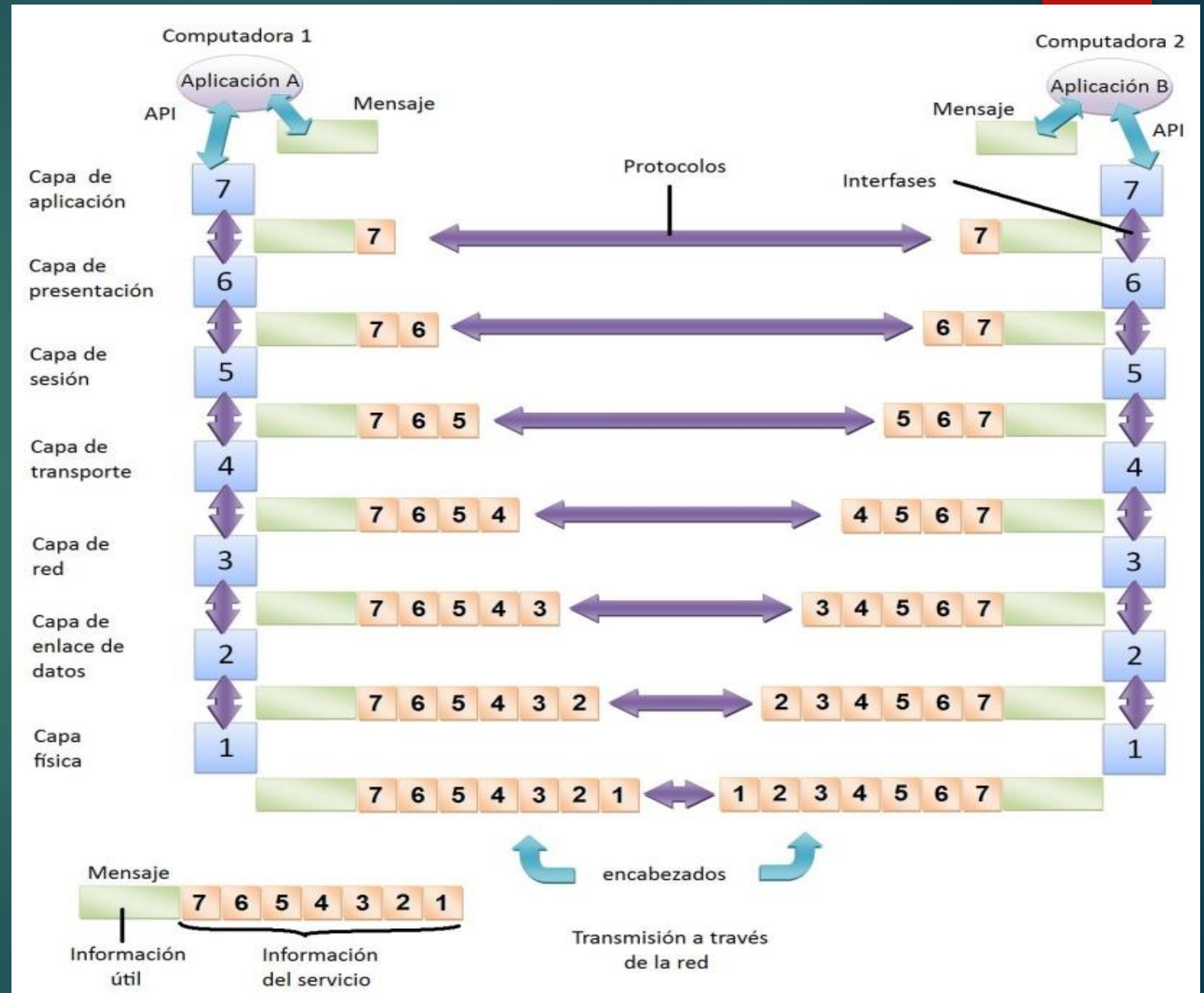
Cualquier sistema (computadora, red de computadoras, sistema operativo, software de aplicación o cualquier otro hardware y software) diseñado de acuerdo a especificaciones que se publican, están disponibles y cumplen con los estándares acordados después de un estudio minucioso y variado que incluya a todas las instancias interesadas.

Sistema abierto

Diseño de redes:

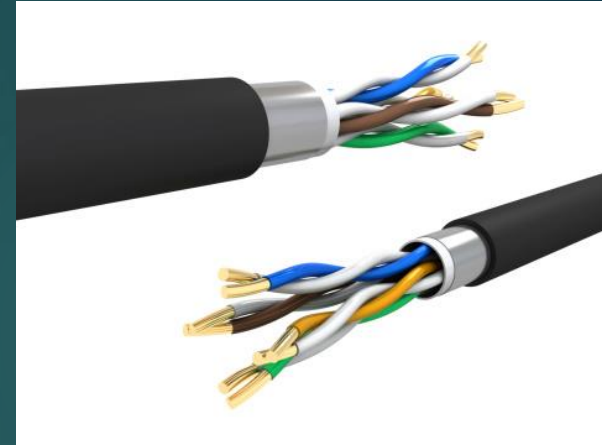
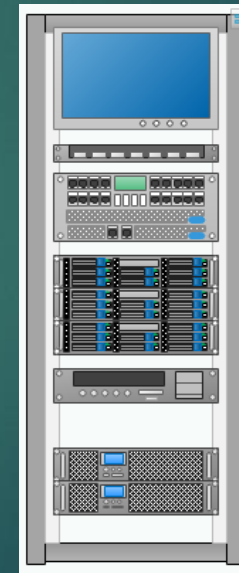
- Posibilidad de construir una red con base en HW y SW de diversos fabricantes que soporten el mismo estándar.
- Posibilidad de reemplazar componentes específicos de la red por unos más avanzados. (costo)
- Posibilidad de interconectar las redes de una manera sencilla.
- Mantenimiento de la red fácil y simple.

Modelo OSI



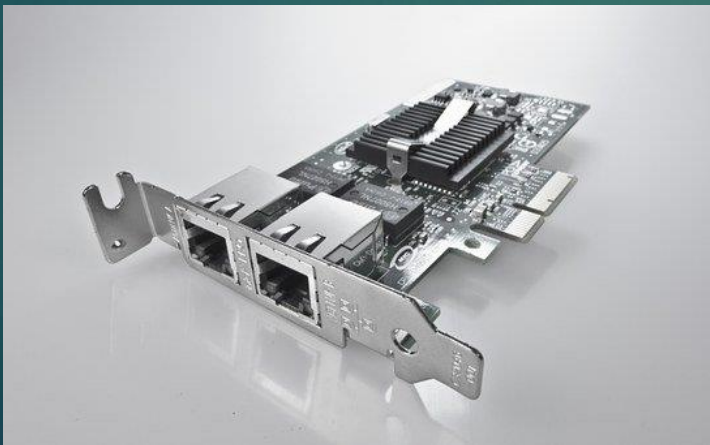
Capa Física

Los aspectos de diseño implican asegurarse de que cuando un lado envía **un bit 1**, éste se reciba en el **otro lado como tal, no como bit 0**. Los aspectos de diseño tienen que ver mucho con las interfaces **mecánicas, eléctricas y de temporización, además del medio físico de transmisión.**



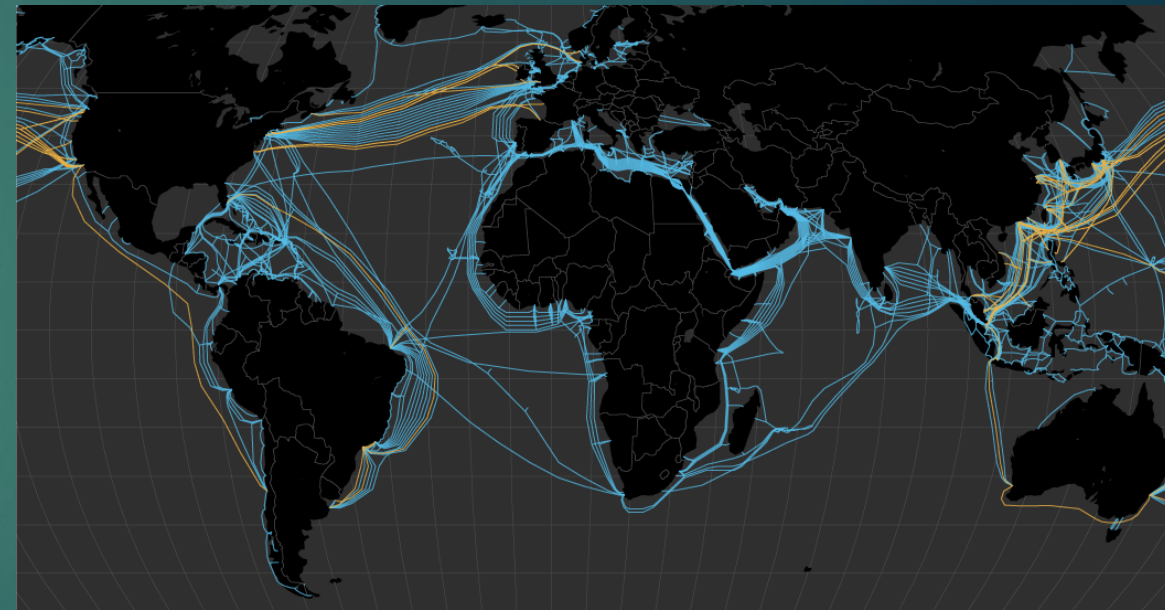
Capa de enlace de datos

Transformar un medio de transmisión puro en una línea de comunicación entre puntos adyacentes, además de que al llegar a la capa de red, aparezca **libre de errores** de transmisión. Logra esta tarea haciendo que el emisor fragmente los datos de entrada en **tramas de datos** y transmitiendo éstas de manera secuencial.



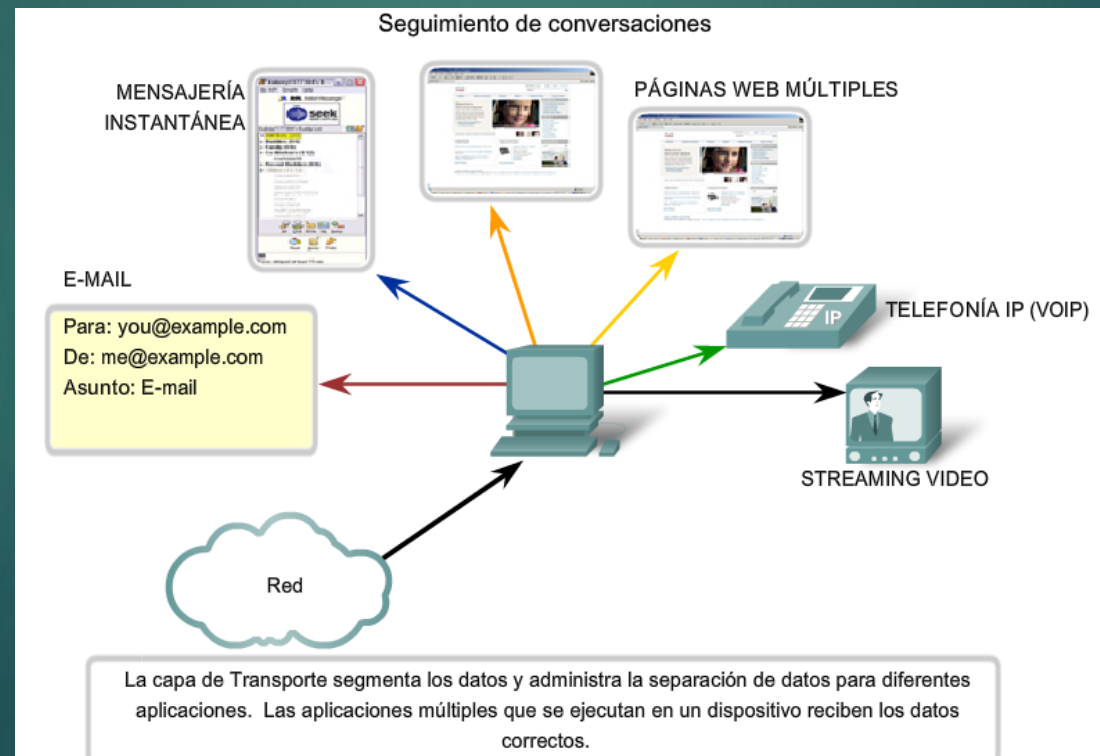
Capa de red

Un aspecto clave del diseño es determinar como se encaminan los paquetes desde su **origen a su destino**, las rutas pueden estar basadas en tablas estáticas (encaminamiento estático) codificadas en la red y que rara vez cambian o en rutas adaptables (encaminamiento dinámico).

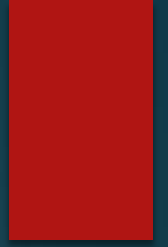


Capa de transporte

- La capa de transporte determina principalmente **qué tipo de servicio** proporcionar a la capa de sesión y, finalmente, a los usuarios de la red.



Capa de sesión

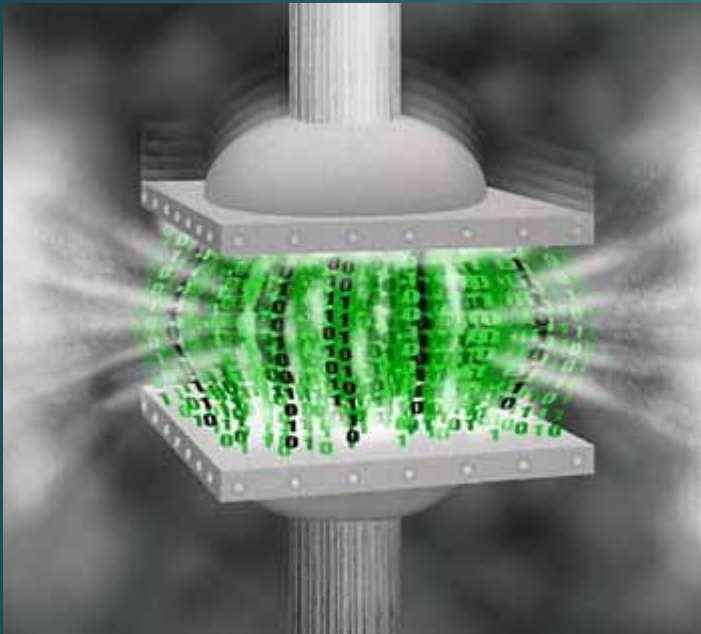


Esta capa permite que los usuarios de máquinas diferentes establezcan sesiones entre ellos. Las sesiones ofrecen varios servicios, como:

- ▶ **Control de diálogo**
- ▶ **Administración de token**
- ▶ **Sincronización**

Capa de presentación

A esta capa le corresponde la **sintaxis** y la **semántica** de la información transmitida.



Capa de aplicación

Esta capa contiene varios protocolos que los usuarios requieren. Un protocolo de aplicación de amplio uso es **HTTP (Protocolo de Transferencia de Hipertexto)**.

Otros protocolos de aplicación se utilizan para la transferencia de archivos, correo electrónico entre otros.





Arquitectura de seguridad de OSI estándar 7498-2

SERVICIOS Y MECANISMOS

Arquitectura de seguridad en el modelo OSI

Es necesario un estándar que permita comenzar la tarea de implementar los servicios de seguridad en productos comerciales de modo que no sólo un **sistema pueda comunicarse con otro**, sino que además pueda hacerlo con la **adecuada seguridad**.



Servicios de seguridad



Servicio de autenticación: Corrobora la veracidad de la fuente de una unidad de datos.

Servicio de control de acceso: Se utiliza para evitar el uso no autorizado de los recursos.

Servicio de confidencialidad de datos: Proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación.

Servicios de seguridad



Servicio de integridad de datos: Garantiza que los datos recibidos por el receptor de una comunicación coinciden con los enviados por el emisor.

Servicio de no repudio: Proporciona la prueba ante una tercera parte de que cada una de las entidades comunicantes que han participado en una comunicación.

Mecanismos de seguridad

Los mecanismos de seguridad son específicos y generalizados.
Mecanismos de seguridad específicos.



Mecanismo de cifrado: Se utiliza para proteger la confidencialidad de los datos ya sea en reposo o en flujo, así como para dar soporte o complementar otros mecanismos de seguridad.

Mecanismos de firma digital: Se emplean para proporcionar una analogía electrónica a la firma manuscrita en documentos electrónicos; de forma similar a las firmas manuscritas, las firmas digitales no deben ser falsificables.

Mecanismos de seguridad específicos



Mecanismo de control de acceso: Se utiliza para autenticar las capacidades de una entidad, con el fin de asegurar los derechos de acceso a recursos que posee.

Mecanismo de integridad de datos: Se encargan de proteger la integridad de los datos, de los paquetes de datos, de las secuencias de los paquetes de datos, así como de los campos correspondientes a dichas secuencias.

Mecanismos de seguridad específicos



Mecanismo de intercambio de autenticación: Su finalidad es verificar la identidad de las entidades en comunicación antes de iniciar el intercambio de información. Autenticación simple y fuerte.

Mecanismo de relleno de tráfico: Se utiliza para brindar protección contra ataques de análisis de tráfico. El término relleno de tráfico se refiere a la generación de ejercicios de comunicación espurios, paquetes de datos espurios, y de datos espurios dentro de dichos paquetes. El objetivo es no revelar si los datos que se están transmitiendo representan y codifican realmente información.



Mecanismos de seguridad específicos



Mecanismo de control de encaminamiento: Permite la selección dinámica o preestablecida de rutas específicas para la transmisión de los datos.

Mecanismo de certificación: Su función es asegurarse de ciertas propiedades de los datos que se comunican entre dos o más entidades, entre los que destacan su integridad, origen, tiempo o destino.

No son específicos de un servicio en particular, y en algunos casos pueden ser contemplados también como aspectos de la gestión de la seguridad.

Mecanismo de funcionalidad de confianza: Se trata de poner en práctica un concepto que se utiliza para ampliar o extender otros mecanismos de seguridad o para establecer su efectividad.

Mecanismo de etiquetas de seguridad: Mecanismo asociado directamente con los recursos del sistema, ya que un nivel de seguridad puede implicar datos adicionales que se asocian a los datos transmitidos o puede ser implícito, y su uso primordial se da en los datos en tránsito.



Mecanismos de seguridad

Mecanismo de detección de eventos: Se trata de un mecanismo relevante para la seguridad ya que su función es detectar violaciones aparentes de la seguridad.



Mecanismo de rastreo de auditoría de seguridad: Se encarga de la revisión de examen independiente de los registros y las actividades del sistema para probar la operatividad de los controles, asegurar el cumplimiento de las políticas y procedimientos operacionales establecidos y recomendar los cambios adecuados en el control, política y procedimientos.

Mecanismos de recuperación de seguridad: Se relaciona directamente con mecanismos gestores de eventos y funciones de gestión, y se encarga de realizar acciones de recuperación con base en las políticas de seguridad establecidas.



Modelo TCP/IP

COMPARACIÓN CON EL MODELO OSI

Pila de protocolos TCP/IP

Como la pila de protocolos TCP/IP fue originalmente desarrollada para Internet, tiene muchas ventajas sobre otros protocolos, en especial cuando se trata de construir redes que incluyen enlaces WAN. Otra ventaja es el sistema de direccionamiento flexible. Esta propiedad también promueve el uso del protocolo en el diseño de redes heterogéneas de gran tamaño.

5,6 y 7

Capa de aplicación

HTTP, SNMP, FTP, Telnet, SMTP, TFTP

4

Capa de transporte

TCP, UDP

3

Capa de internet (red)

IP, ICMP, RIP, OSPF

1 y 2

Capa de acceso a la red

Ethernet, Token Ring, X.25

Capa de aplicación

Corresponde a las 3 capas superiores del modelo OSI: las de aplicación, presentación y sesión; además combina los servicios proporcionados por el sistema a las aplicaciones del usuario.

5,6 y 7

Capa de aplicación

HTTP, SNMP, FTP, Telnet, SMTP, TFTP

4

Capa de transporte

TCP, UDP

3

Capa de internet (red)

IP, ICMP, RIP, OSPF

1 y 2

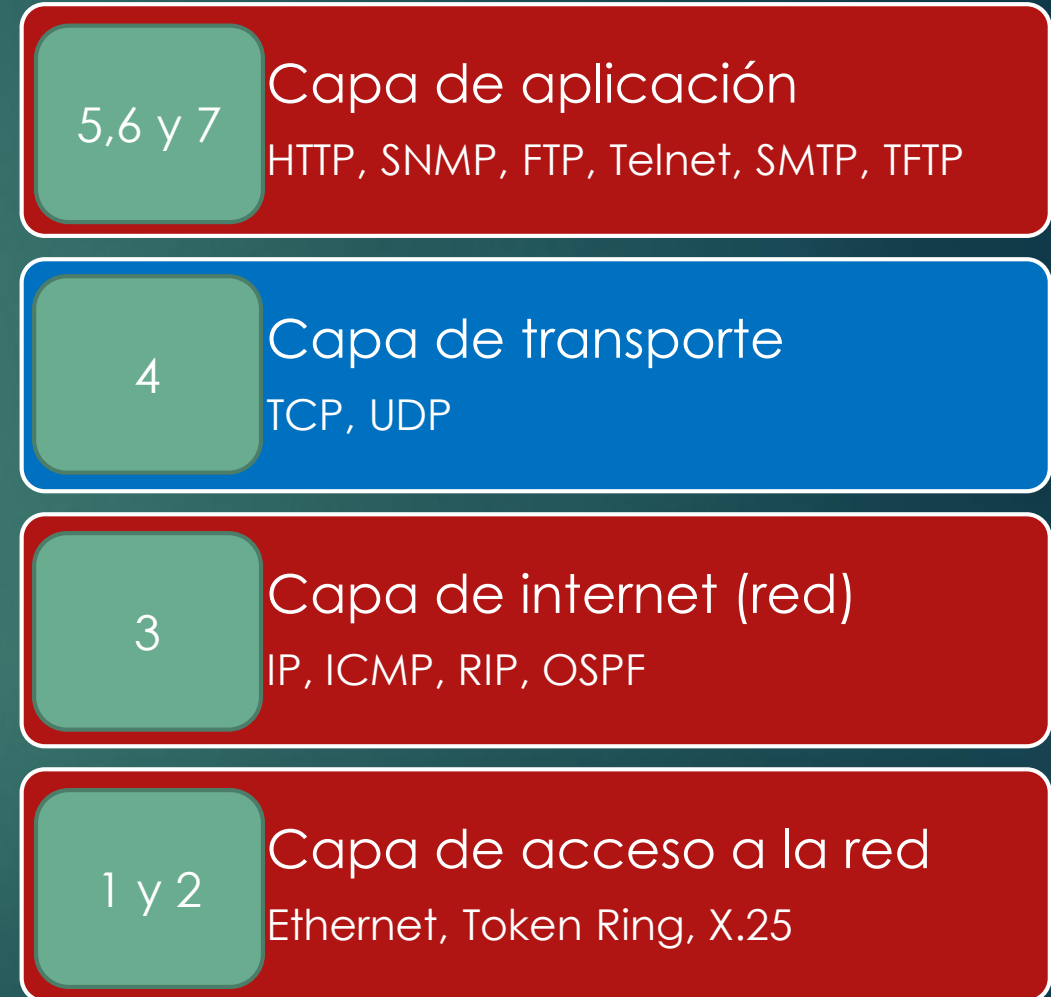
Capa de acceso a la red

Ethernet, Token Ring, X.25

Capa de transporte

Puede proporcionar los dos tipos de servicios siguientes de la capa superior:

- ▶ Entrega garantizada: protocolo de control de la transmisión (TCP)
- ▶ Entrega con el mejor esfuerzo: protocolo de datagrama del usuario (UDP)



Capa de red

Las funciones de esta capa corresponden a las de la capa de red del modelo OSI y aseguran la transferencia de paquetes dentro de la interred la cual se crea mediante la conexión de varias redes.

- **El protocolo Internet (IP)** es el más importante. Entre sus funciones se encuentra el envío de paquetes entre redes (de un router a otro) hasta que el paquete llegue a la red a la que está destinado.

5,6 y 7

Capa de aplicación

HTTP, SNMP, FTP, Telnet, SMTP, TFTP

4

Capa de transporte

TCP, UDP

3

Capa de internet (red)

IP, ICMP, RIP, OSPF

1 y 2

Capa de acceso a la red

Ethernet, Token Ring, X.25

Capa de acceso a la red

- ▶ Es responsable de organizar la interacción con las tecnologías de red utilizadas en las redes que forman la interred. Corresponde a las capas de enlace de datos y física del modelo OSI.
- ▶ Esta capa no está regulada, es decir, soporta todas las tecnologías de red más comunes.

5,6 y 7

Capa de aplicación

HTTP, SNMP, FTP, Telnet, SMTP, TFTP

4

Capa de transporte

TCP, UDP

3

Capa de internet (red)

IP, ICMP, RIP, OSPF

1 y 2

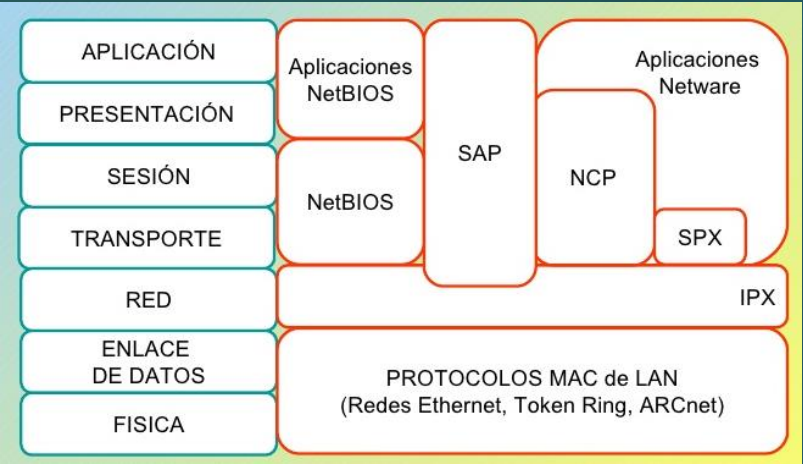
Capa de acceso a la red

Ethernet, Token Ring, X.25

Otros modelos

SNA
NIVEL 7.SERVICIOS DE TRANSACCIONES (Transaction Services)
NIVEL 6.SERVICIOS DE PRESENTACION (Presentation Services)
NIVEL 5.CONTROL DE FLUJO DE DATOS (Data Flow Control)
NIVEL 4.CONTROL DE TRANSMISION (Transmission Control)
NIVEL 3.CONTROL DE CAMINO (Path Control)
NIVEL 2.CONTROL DE ENLACE DE DATOS (Data Link Control)
NIVEL 1.FISICO (Physical Control)

SNA de IBM 1974



Novell Network 1983

OSI Layer	Protocols
Application	AppleShare
Presentation	AppleTalk Filing Protocol (AFP)
Session	Zone Information Protocol (ZIP), AppleTalk Session Protocol (ASP), AppleTalk Data Stream Protocol (ADSP), Password Authentication Protocol (PAP)
Transport	AppleTalk Echo Protocol (AEP), Name Binding Protocol (NBP), AppleTalk Transaction Protocol (ATP), Routing Table Maintenance Protocol (RTMP)
Network	Datagram Delivery Protocol (DDP)
Data Link	LocalTalk, EtherTalk, TokenTalk, FDDITalk
Physical	Physical transmission media (coax, twisted-pair, fiber-optic)

Apple Inc. 1985