



# Tema 1. Introducción a las redes de datos

Introducción a las redes de ordenadores

Boni García  
Curso 2017/2018

# Índice de contenidos

---

1. Introducción
2. ¿Qué es Internet?
3. Un poco de historia
4. Tipos de redes
5. Modelos de referencia
6. Análisis de Protocolos

# Índice de contenidos

---

1. Introducción
  - Conceptos generales
  - Objetivo de las redes de datos
  - Arquitectura de comunicación en niveles
  - Organismos de estandarización
2. ¿Qué es Internet?
3. Un poco de historia
4. Tipos de redes
5. Modelos de referencia
6. Análisis de protocolos

# 1. Introducción

---

## Conceptos generales

- **Red de ordenadores = red de datos = red telemática:** Es un tipo de *red de telecomunicación* en la que se transmiten datos (información binaria). Se conocen así en contraposición a las redes de voz, que son históricamente las primeras redes de telecomunicación



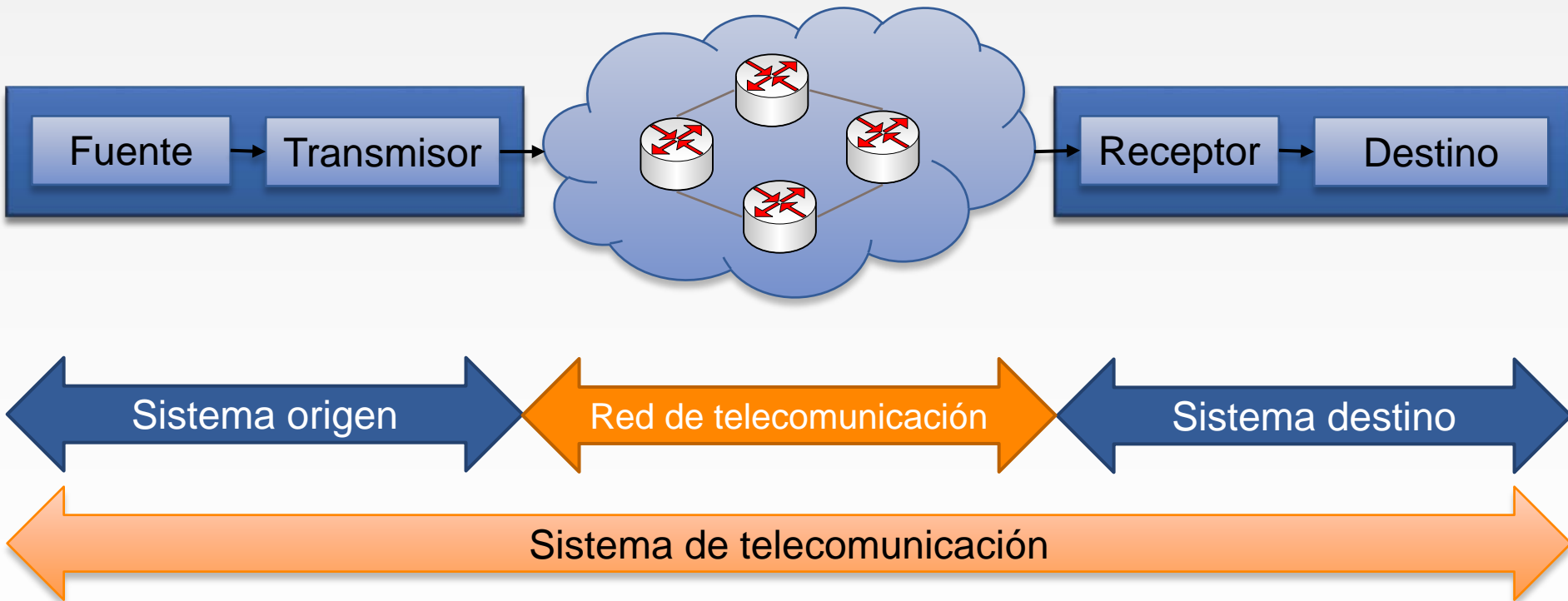
- **Red de telecomunicación:** Conjunto de nodos y medios de transmisión necesarios para el intercambio de información en un *sistema de telecomunicación*



- **Sistema de telecomunicación:** Sistema que permite la comunicación remota entre un sistema origen y otro destino

# 1. Introducción

## Conceptos generales



# 1. Introducción

---

## Conceptos generales

- **Canal de comunicaciones:** medio de transmisión por el que viajan las señales portadoras de información entre el sistema origen y destino. Según la capacidad de transmisión, un canal puede ser:

- *Full duplex:* comunicación bidireccional y simultánea



- *Half duplex:* comunicación bidireccional pero no simultánea



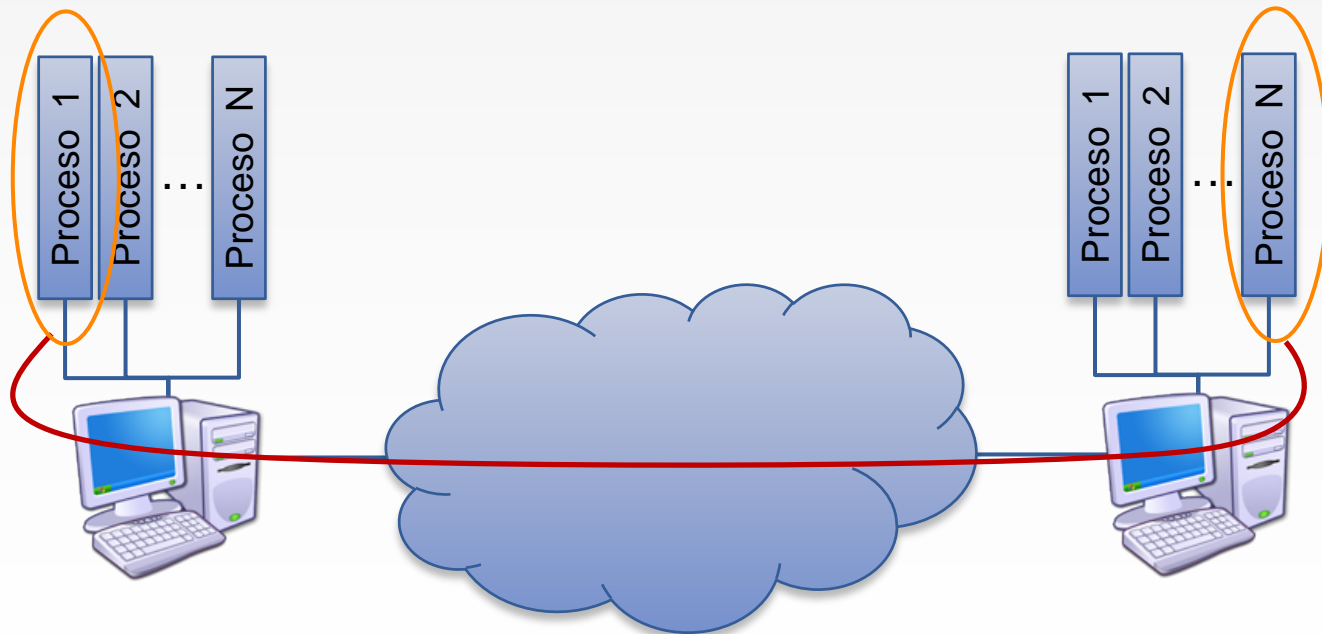
- *Simplex:* comunicación unidireccional



# 1. Introducción

## Objetivo de las redes de datos

- Las redes de datos sirven para comunicar procesos (programas en ejecución) remotos, dando lugar a los que se conoce como **servicio distribuido** o **servicio telemático**



# 1. Introducción

---

## Arquitectura de comunicación en niveles

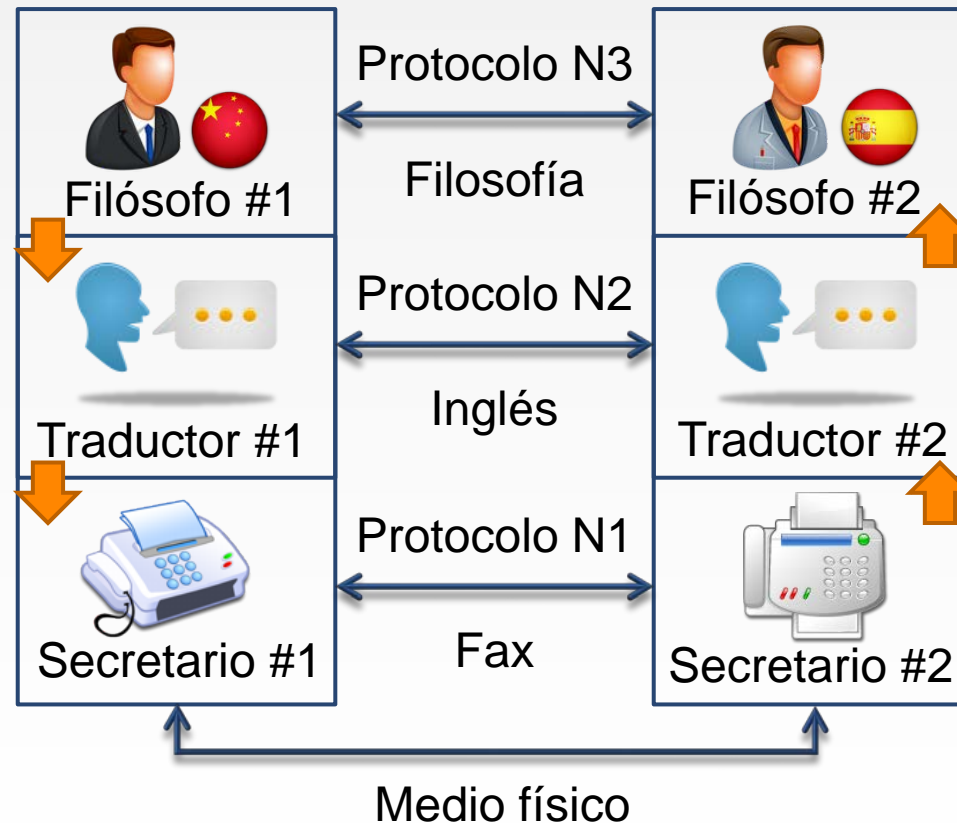
- Para lograr este objetivo se usa una arquitectura de comunicación estratificado en **niveles**
- Se basa en el principio “*divide y vencerás*”
  - Dividimos el problema en diferentes niveles de abstracción de forma que el problema global se pueda resolver por partes
  - Cada nivel se construye sobre el anterior
- Hay dos conceptos fundamentales en una arquitectura de comunicación estratificada en nivel:
  - **Servicio**: conjunto de operaciones que un nivel ofrece al superior
  - **Protocolo**: conjunto de reglas que definen la comunicación entre elementos del mismo nivel (entidades)



# 1. Introducción

## Arquitectura de comunicación en niveles

- Analogía:



# 1. Introducción

---

## Arquitectura de comunicación en niveles

### ■ Servicio

- Es el conjunto de operaciones (**primitivas**) que una entidad de nivel N ofrece a la entidad de nivel N+1
- Una entidad de nivel N utiliza los servicios proporcionados por la entidad N-1
- Los servicios están disponible a través de su **interfaz**, y tiene una **dirección** única que lo identifica

### ■ Protocolo

- Es el conjunto de reglas (formato mensajes, orden, acciones a realizar) que permiten que dos o más entidades de un sistema se comuniquen
- Una **entidad** es un elemento que implementa el protocolo. Las entidades del mismo nivel se llaman *entidades pares*
- Las unidades de datos que se intercambian las entidades pares se conocen como **PDU** (*Protocol Data Unit*)

# 1. Introducción

---

## Organismos de estandarización

- Para que un modelo de comunicación en niveles sea efectivo debe ser adoptado por los diferentes participantes en la comunicación
- Para ello, existen diferentes organismos que promueven **estándares**
- Organismos de estandarización en el ámbito de las redes de datos (networking)
  - *International Organization for Standardization (ISO)*
  - *Institute of Electrical and Electronics Engineers (IEEE)*
  - *International Telecommunication Union - Telecommunication Standardization Sector (ITU-T)*
  - *American National Standards Institute (ANSI)*
  - *European Telecommunications Standards Institute (ETSI)*

# 1. Introducción

---

## Organismos de estandarización

- El organismos de estandarización en el ámbito de Internet es la ISoc (*Internet Society*). Está dividido en:
  - *Internet Architecture Board (IAB)*: Supervisión y aprobación de normas
  - *Internet Engineering Steering Group (IESG)*: Coordinación
  - *Internet Engineering Task Force (IETF)*: Especificación de estándares
  - *Internet Assigned Number Authority (IANA)*: Asignación de recursos
- Los documentos asociados a estos estándares IETF se conocen como documentos **RFC** (*Request For Comments*)

# Índice de contenidos

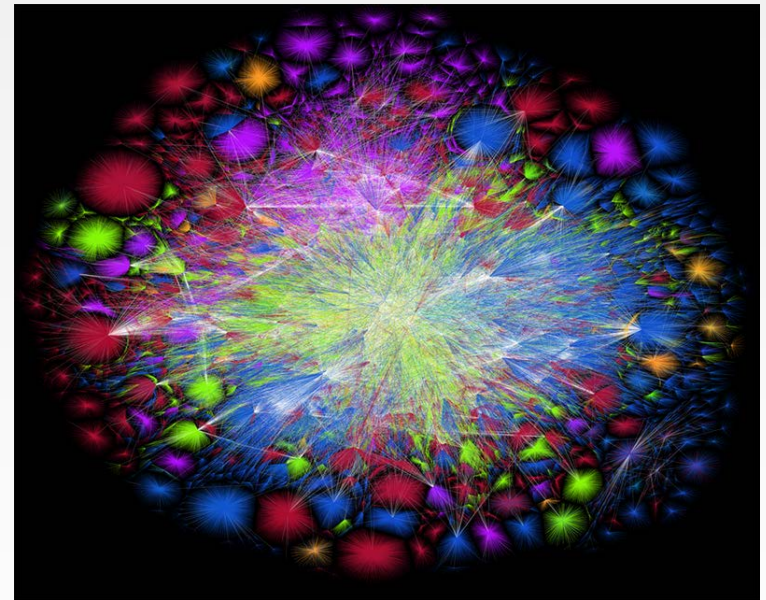
---

1. Introducción
2. ¿Qué es Internet?
  - Redes troncales
  - Proveedores de servicio
  - Redes de acceso
  - Conexiones entre proveedores
  - Neutralidad de la red
3. Un poco de historia
4. Tipos de redes
5. Modelos de referencia
6. Análisis de protocolos

## 2. ¿Qué es Internet?

---

**Internet** es un conjunto descentralizado de redes de datos interconectadas que utilizan la familia de protocolos **TCP/IP** que interconecta cientos de millones de dispositivos (**hosts** o **sistemas terminales**) a lo largo de todo el mundo



<http://www.opte.org/>

Internet = *red de redes*

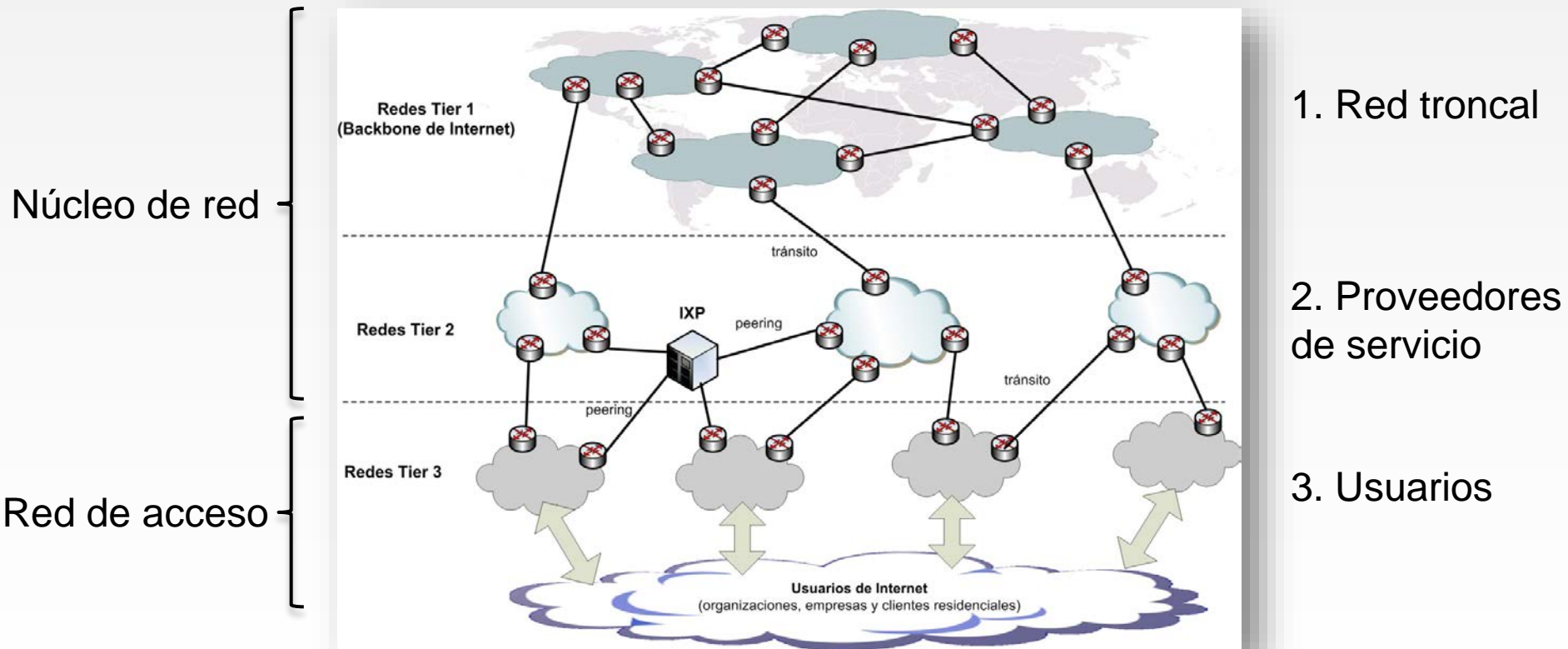
## 2. ¿Qué es Internet?

---

- Los elementos básicos de Internet son:
  - Equipos terminales (**hosts**): Tradicionalmente son ordenadores PC, estaciones de trabajo, servidores de red, televisores, consolas, teléfonos móviles, webcams, etc.
  - **Enlaces**: Conectan a los hosts usando diferentes medios físicos: cable coaxial, par de cobre, fibra óptica y el espectro de radio
  - Conmutadores. Sistemas que reenvía los paquetes de información que llegan a su entrada a uno de sus enlaces de comunicaciones de salida. Los tipos más utilizados son los **routers**
- Los mensajes que intercambian los hosts en Internet se dividen en paquetes binarios que viajan a través de enlaces y routers

## 2. ¿Qué es Internet?

### Estructura de Internet





## 2. ¿Qué es Internet?

---

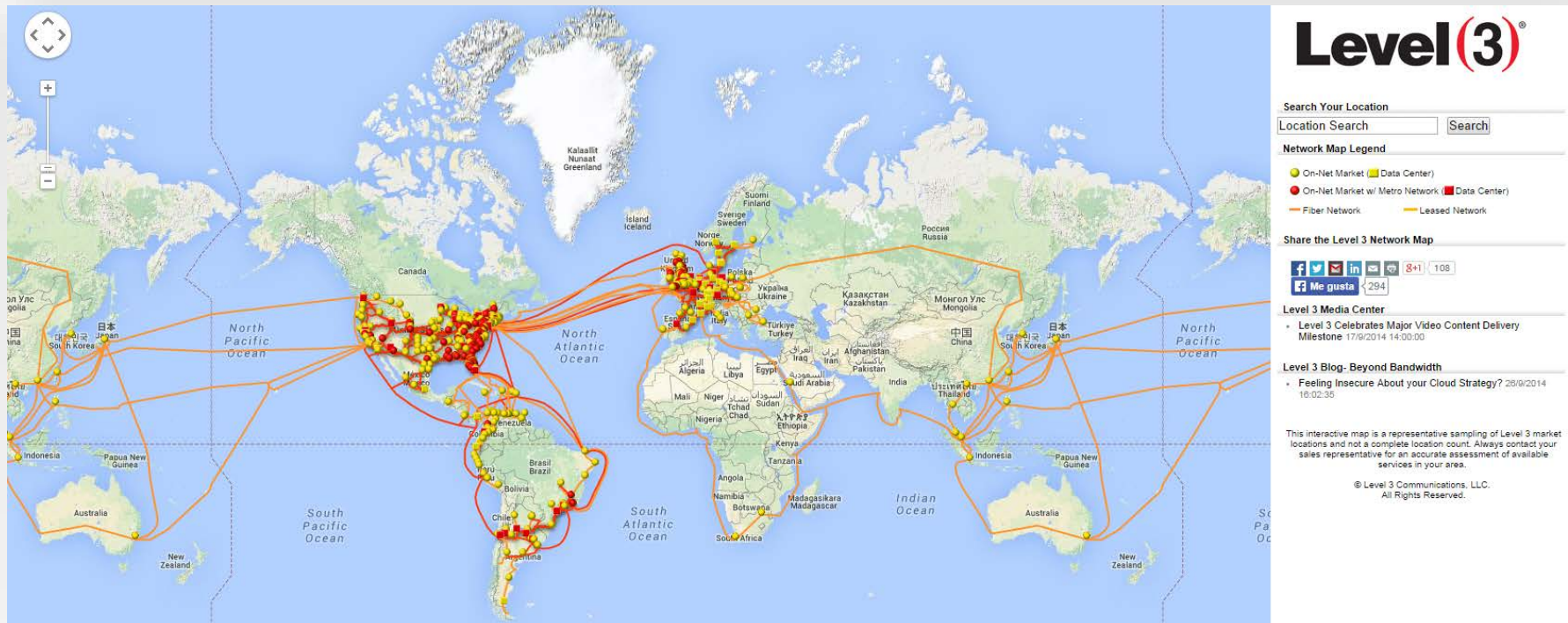
### Redes troncales

- La **redes troncales** (*backbone*) de Internet están compuestas de un gran número de routers interconectados mediante cables de fibra óptica
- Los routers de la redes troncal se conocen como **core routers**
  - Proporcionan cobertura internacional
  - Pueden conectar con cualquier máquina en Internet sin necesitar de ningún acuerdo con terceros
  - Están conectados a un gran número de routers de nivel 2
- Las empresas que gestionan los routers de nivel 1 son
  - Sprint, Verizon, MCI (anteriormente UUNet/WorldCom), AT&T, NTT, Level3, Qwest y Cable & Wireless
  - Oficialmente, no existe ningún grupo que conceda este estatus

## 2. ¿Qué es Internet?

### Redes troncales

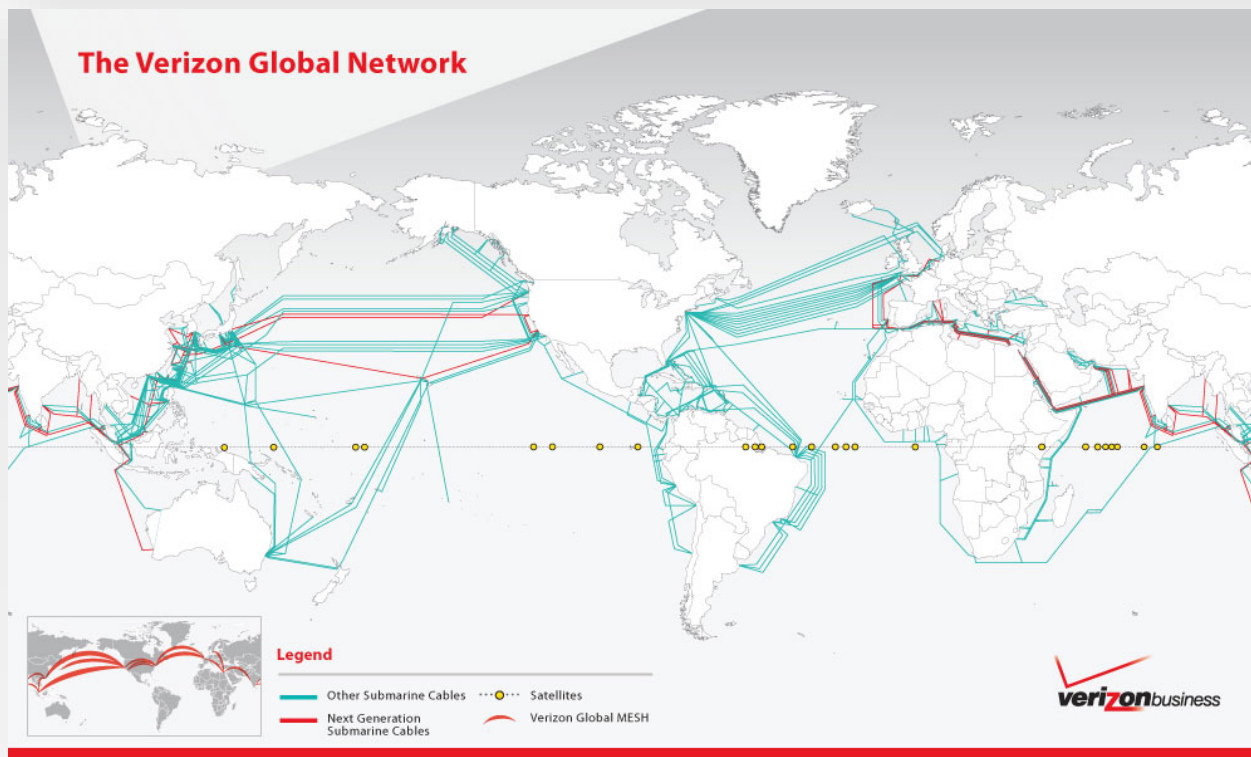
- Backbones de Internet (Level3)



## 2. ¿Qué es Internet?

### Redes troncales

- Backbones de Internet (Verizon)



## 2. ¿Qué es Internet?

### Redes troncales

- Backbones de Internet (NTT)



## 2. ¿Qué es Internet?

---

### Proveedores de servicio

- Los sistemas terminales acceden a Internet a través de **ISP** (*Internet Service Provider*)
- Los ISP son empresas que proporcionan acceso a Internet a sus clientes
- Por regla general, un ISP de nivel 2 tiene cobertura regional o nacional
- Ejemplos de ISPs en España: Movistar, Vodafone, Orange, Yoigo, Ono, Jazztel, Telecable, Euskaltel, etc...

## 2. ¿Qué es Internet?

---

### Redes de acceso

- Los usuarios se sitúan en lo que se conoce como *frontera de Internet*
- Las tecnologías principales de acceso a Internet son:
  - Acceso telefónico
  - DSL (*Digital Subscriber Line*)
  - Cable
  - Fibra óptica (FTTH, *Fiber To The Home*)
  - Satélite
  - Redes móviles (3G/4G)



## 2. ¿Qué es Internet?

---

### Conexiones entre proveedores

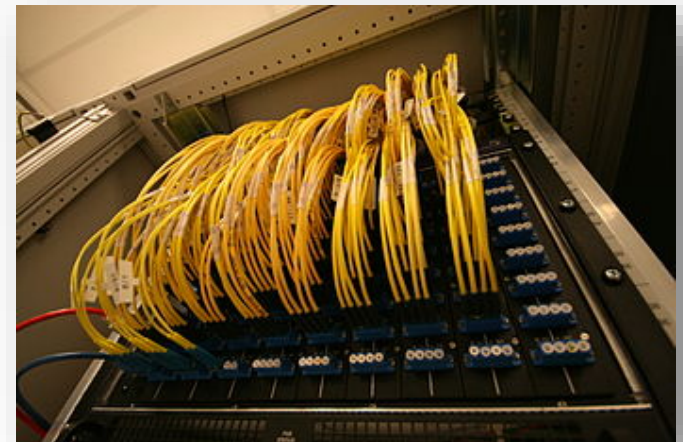
- Hay dos tipos de conexiones entre operadores (del mismo o diferente nivel):
  1. **Conexiones de tránsito.** Conexión entre operadores de diferente jerarquía. El operador de mayor jerarquía (proveedor) vende una conexión de tránsito al operador de menor jerarquía (cliente)
  2. **Conexión de *peering*.** Conexión utilizada para el intercambio de tráfico sin coste entre dos operadores del mismo nivel. Puede ser de dos tipos:
    - Públicos: utilizando un punto neutro
    - Privados: conexión directa entre los dos proveedores

## 2. ¿Qué es Internet?

---

### Conexiones entre proveedores

- Un **punto neutro** (IXP, *Internet Exchange Point*, también llamados NAP, *Network Access Point*) es una infraestructura física que permite a diferentes ISP intercambiar tráfico
- Lista completa de IXPs: <https://www.euro-ix.net/ixps/list-ixps/>
- Actualmente en España existen los siguientes puntos neutros:
  - ESPANIX (Madrid)
  - EuskoNIX (San Sebastián)
  - CATNIX (Barcelona)
  - GalNIX (Santiago de Compostela)
  - NAP de las Américas - Madrid (Madrid)
  - MadIX (Madrid)







## 2. ¿Qué es Internet?

---

### Neutralidad de la red

- La neutralidad de la red (*net neutrality*) es un principio por el cual todo el tráfico de datos en Internet se debe tratar por igual, independientemente de su contenido u origen
- Este principio está ligado a Internet desde sus comienzos
- Lo aplican las entidades reguladoras (gobiernos) y lo deben cumplir principalmente los proveedores de servicio (ISP)
- Ejemplo de no respetar el principio de neutralidad de la red: en 2008 el ISP norteamericano Comcast redujo la velocidad de subida de aplicaciones que usaban P2P para compartir ficheros

# Índice de contenidos

---

1. Introducción
2. ¿Qué es Internet?
3. **Un poco de historia**
4. Tipos de redes
5. Modelos de referencia
6. Análisis de protocolos

## 3. Un poco de historia

---

- 1958 – DARPA (*Defense Advanced Research Projects Agency*)
  - Agencia del Departamento de Defensa de EEUU responsable del desarrollo de nuevas tecnologías para uso militar.
  - Fue creada como consecuencia tecnológica de la Guerra Fría
  - En este departamento que surgieron los fundamentos de ARPANET, red que dio origen a Internet.



## 3. Un poco de historia

---

- Años 60 - Arpanet (*Advanced Research Projects Agency*)
  - El mito es que fue un sistema de comunicaciones que pudiese sobrevivir a un ataque nuclear → **conmutación de paquetes**
  - Algunos opinan que simplemente fue diseñada para tolerar fallos
  - Red de comunicaciones no centralizada (si algunos nodos fueran destruidos/fallasen los paquetes podrían seguir otro camino)
  - Comienza a funcionar con enlace entre 4 cuatro centros de investigación independientes (DARPA, la corporación RAND, el MIT y NPL en el Reino Unido)



## 3. Un poco de historia

---

### ■ Años 70

- 1971: Ray Tomlison creó el correo electrónico
- Modelo de documentos de conclusiones y trabajos (**RFCs**)



### ■ Años 80

- Boom de los ordenadores personales y redes de área local
- 1982: Formalización de la pila de protocolos TCP/IP
- 1983: Nace oficialmente **Internet** al separarse MILNET (parte militar) de ARPANET
- 1984: DNS (*Domain Name Service*)
- 1987: La red alcanza los 20.000 ordenadores
- 1988: Primer virus en la red

## 3. Un poco de historia

---

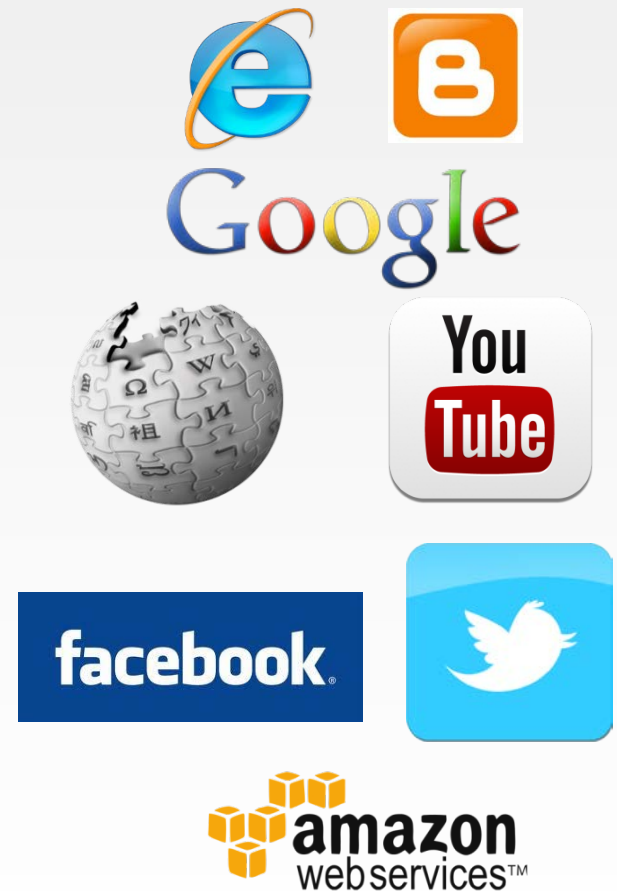
- 1989
  - Tim Berners-Lee del CERN (*Conseil Européen pour la Recherche Nucléaire*), propone un primer esbozo para la WWW (*World Wide Web*)
  - Berners-Lee y su equipo escriben el primer servidor (httpd) y el primer navegador (llamado *WorldWideWeb*)
  - Berners-Lee y su equipo crearon el HTML, el HTTP y las URL
- 1994
  - Nace el W3C (*World Wide Web Consortium*)



## 3. Un poco de historia

---

- 1995: Internet Explorer
- 1997: Blog
- 1998: Google
- 2001: Wikipedia
- 2005: YouTube
- 2006: Facebook
- 2006: Twitter
- 2008: Amazon Web Services





# Índice de contenidos

---

1. Introducción
2. ¿Qué es Internet?
3. Un poco de historia
4. Tipos de redes
  - Técnicas de conmutación
  - Extensión
  - Topología
5. Modelos de referencia
6. Análisis de protocolos

## 4. Tipos de redes

---

### Técnicas de conmutación

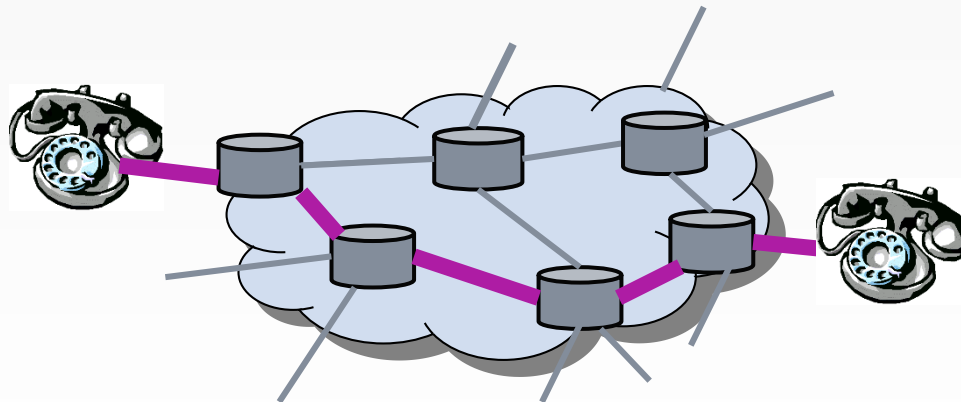
- Las **técnicas de conmutación** (*switching*) definen la manera en que los datos atraviesan el camino entre el nodo origen y el destino
- En función de la **técnica de conmutación** empleada, podemos clasificar las redes de telecomunicación en dos grandes grupos:
  - Red de **conmutación de circuitos**
  - Red de **conmutación de paquetes**

## 4. Tipos de redes

---

### Técnicas de conmutación

- Red de **conmutación de circuitos**
  - Existe un camino dedicado (*circuito*) entre los equipos terminales
  - Toda la información sigue el mismo camino
  - El circuito se establece mediante *señalización*
  - Ejemplo: Red Telefónica Conmutada

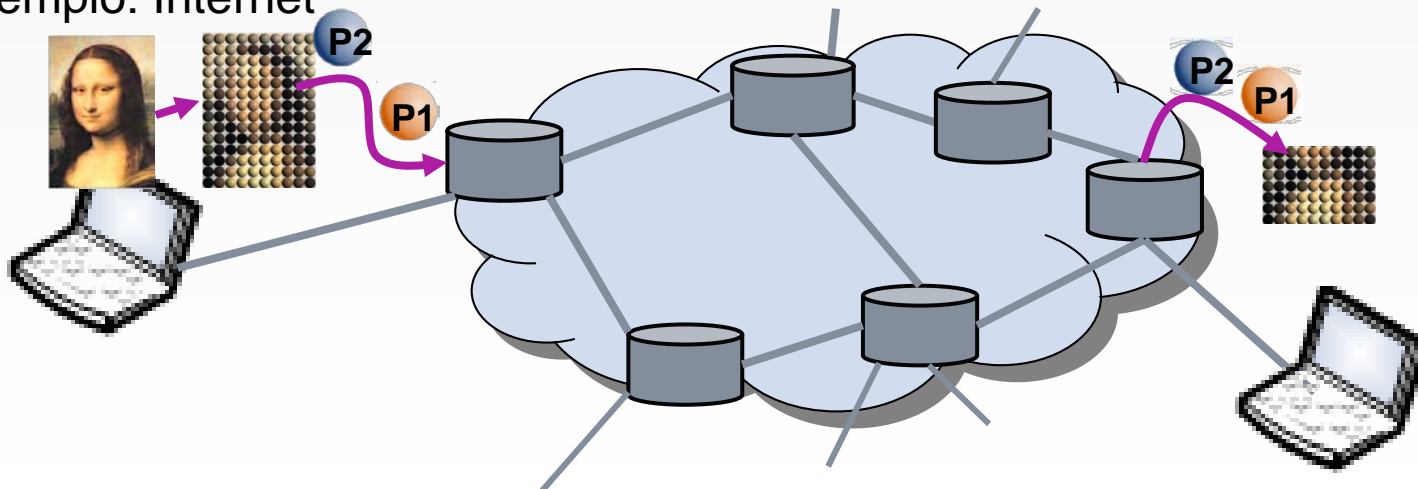


## 4. Tipos de redes

### Técnicas de conmutación

#### ▪ Red de **conmutación de paquetes**

- La información se transmite en forma de **paquetes**
- Los nodos intermedios **almacenan y reenvían** (*store and forward*) los paquetes, encaminando los mismos hasta el destino
- Una vez los paquetes llegan a destino, el mensaje es **reensamblado**
- Ejemplo: Internet







## 4. Tipos de redes

---

### Técnicas de conmutación

- Comparación entre conmutación circuitos y paquetes

Conmutación circuitos	Conmutación paquetes
 Idóneos para servicios de comunicación en tiempo real (por ejemplo llamadas de voz)	 Compartición de recursos más eficiente
 Ineficiencia en la gestión de recursos (circuitos dedicados se usen realmente o no)	 Puede ser inadecuada para los servicios en tiempo real porque los retardos son variables e impredecibles (retardos de cola)

## 4. Tipos de redes

---

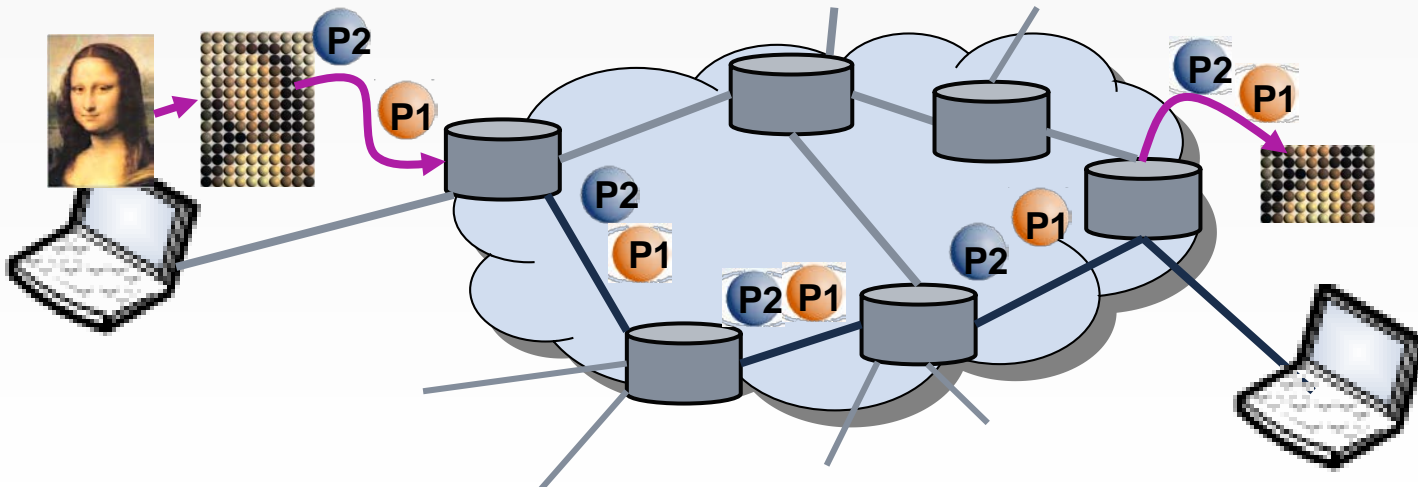
### Técnicas de conmutación

- Hay dos tipos de técnica de conmutación de paquetes:
  1. Conmutación de paquetes **orientado a la conexión**:
    - También llamada circuito virtual
    - Por ejemplo, redes X.25, ATM, Frame Relay
  2. Conmutación de paquetes **no orientado a la conexión**:
    - También llamada técnica de datagramas
    - Por ejemplo: redes IP, como Internet

## 4. Tipos de redes

### Técnicas de conmutación

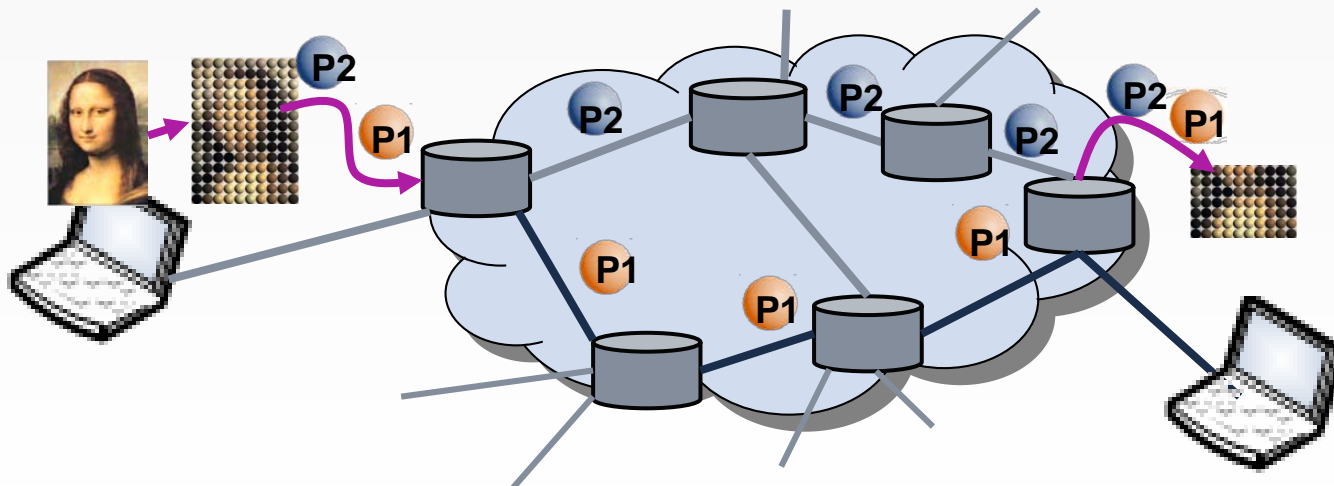
- Red de **conmutación de paquetes orientadas a conexión**
  - Hay tres fases: establecimiento, transferencia y liberación
  - Solo los paquetes de llamada llevan dirección origen y destino
  - La ruta se determina en la fase de establecimiento con el paquete de llamada
  - Todos los paquetes siguen el mismo camino



## 4. Tipos de redes

### Técnicas de conmutación

- Red de **conmutación de paquetes no orientadas a conexión**
  - No hay fases de establecimiento ni liberación
  - Todos los paquetes llevan dirección origen y destino
  - Cada paquete puede seguir una ruta diferente
  - Los paquetes pueden llegar desordenados o incluso perderse





## 4. Tipos de redes

### Técnicas de conmutación

- Comparación redes conmutadas orientadas a y no orientadas a conexión:

Orientadas a la conexión	No orientadas a la conexión
<p>✓ La red proporciona control de errores. Al existir un circuito virtual, los paquetes se envían más rápido (la conmutación se puede hacer incluso por hardware, por ejemplo en ATM)</p>	<p>✓ Muy flexible (si un nodo falla, se pueden encontrar rutas alternativas)</p>
<p>✗ Menos flexible (si un nodo falla, todos los circuitos virtuales de ese nodo fallan)</p>	<p>✗ Puede ser inadecuada para los servicios en tiempo real porque los retardos son variables e impredecibles</p>

## 4. Tipos de redes

---

### Extensión

- LAN (*Local Area Network*), red de área local
  - Redes privadas
  - Pocos kilómetros de extensión (oficina, universidad, etc.)
  - Conectan ordenadores y equipos de una organización
  - Objetivo: compartir recursos e intercambiar información entre ellos.
  - Bajo retardo y pocos errores
  - Limitadas en tamaño y en tiempo de transmisión
  - Intranet = LAN + servicios

## 4. Tipos de redes

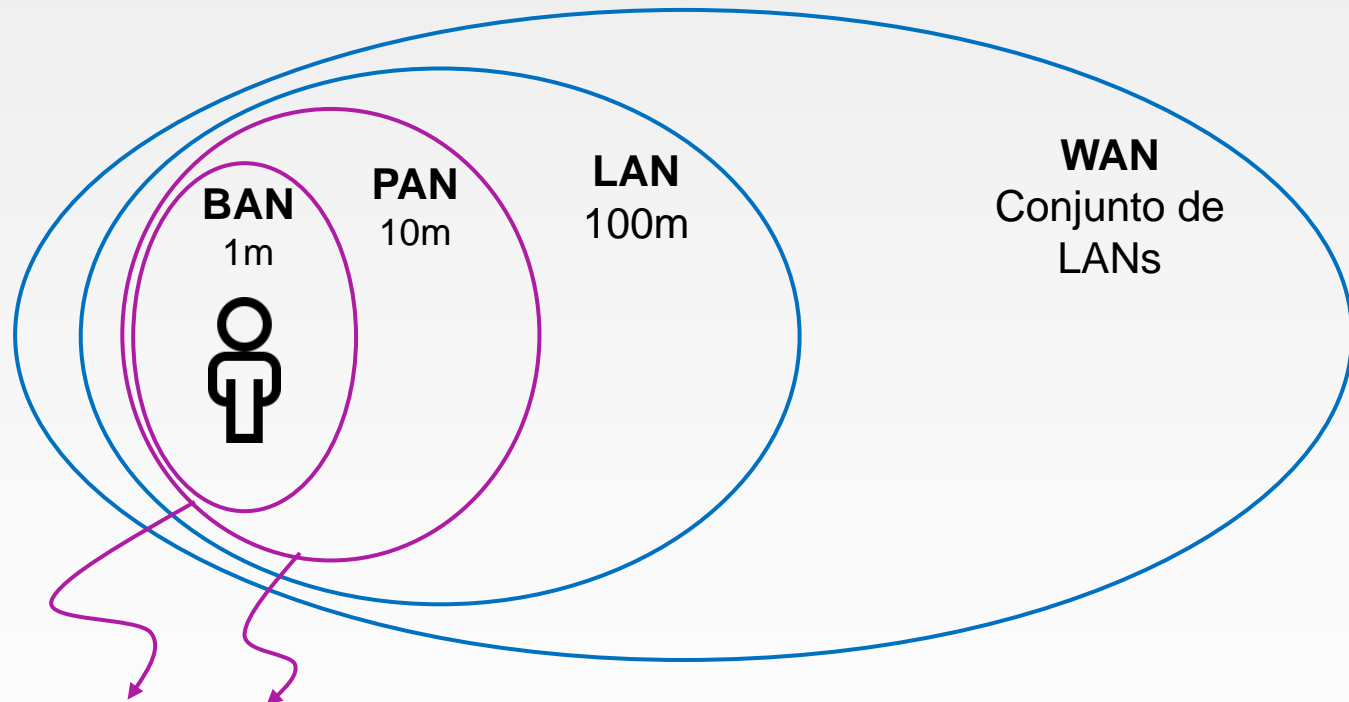
---

### Extensión

- **MAN** (*Metropolitan Area Network*), red de área metropolitana
  - Área geográfica extensa
  - Interconexión de varias LAN
  - Compuesta por líneas de comunicación y nodos (equipos que interconectan redes entre sí)
  
- **WAN** (*Wide Area Network*), red de área extensa
  - Mayor a las MAN
  - interconecta redes y dispositivos en áreas extensas (país, continente)

## 4. Tipos de redes

### Extensión



- Redes para dispositivos que se encuentran muy próximas a la persona (por ejemplo Bluetooth): manos libres, cascos inalámbricos, ...
  - PAN (*Personal Area Network*), red de área personal
  - BAN (*Body Area Network*), red de área corporal

## 4. Tipos de redes

---

### Extensión

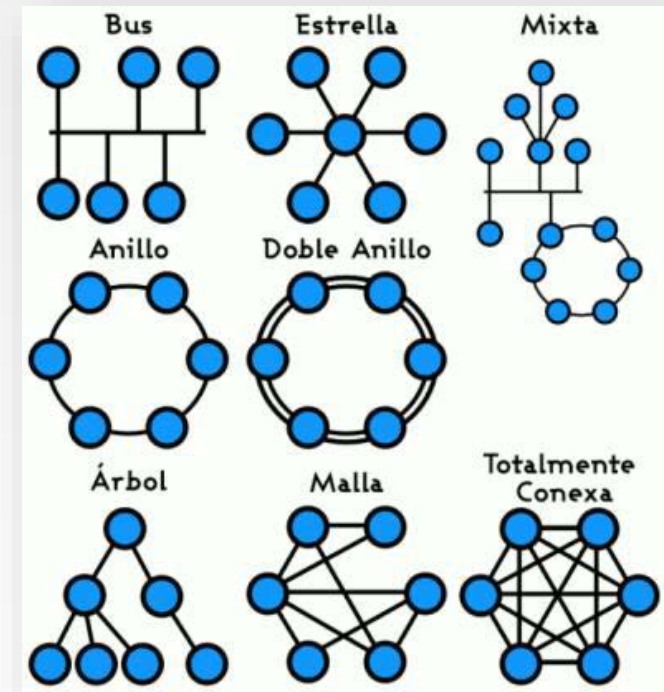
<b>Distancia</b>	<b>Ubicación destino</b>	<b>Tipo de Red</b>
1 m	Uno mismo	Body Area Network (BAN)
10 m	Habitación	Personal Area Network (PAN)
100 m	Hogar	Local Area Network (LAN)
1 km	Campus	Local Area Network (LAN)
10 km	Ciudad	Metropolitan Area Network (MAN)
100 km	País	Wide Area Network (WAN)
1000 km	Continente	Wide Area Network (WAN)
10000 km	Planeta	Internet

---

## 4. Tipos de redes

### Topología

- La **topología** de red describe la forma en que se disponen los enlaces para comunicar a los host de una red. Hay que distinguir dos formas de topología:
  - Topología física: Distribución de los enlaces físicos y equipos. A veces se llama topografía
  - Topología lógica: Describe la forma en las tramas recorren los enlaces de una red



# Índice de contenidos

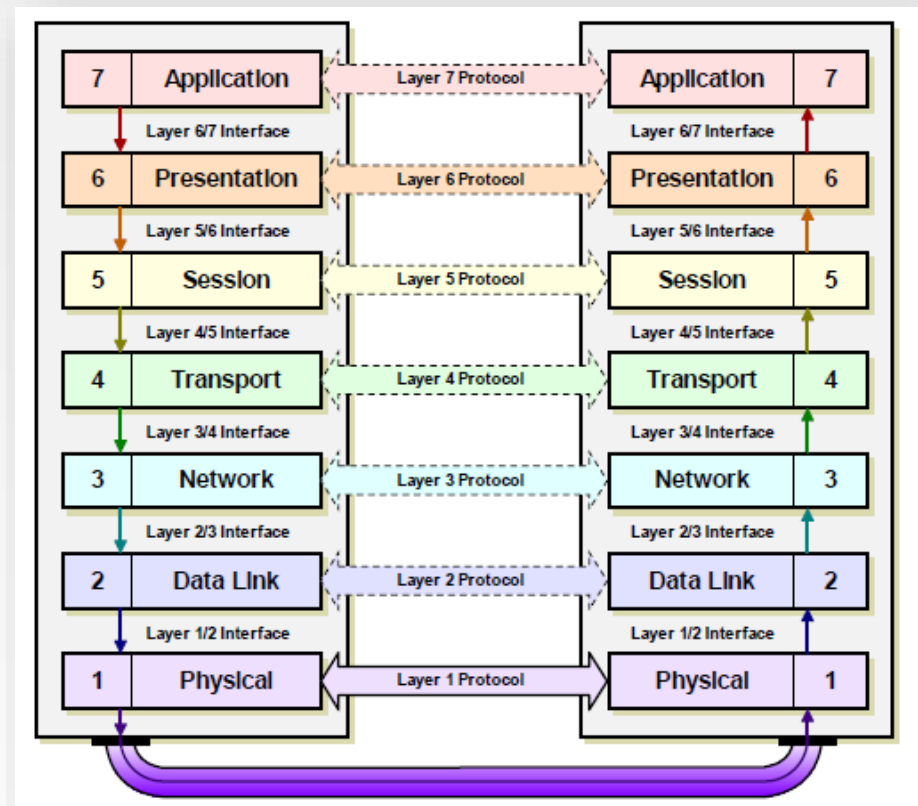
---

1. Introducción
2. ¿Qué es Internet?
3. Un poco de historia
4. Tipos de redes
5. Modelos de referencia
  - El modelo OSI
  - El modelo TCP/IP
6. Análisis de protocolos

## 5. Modelos de referencia

### El modelo OSI

- Modelo OSI (*Open System Interconnection*)
- Modelo de referencia para la interconexión de sistemas abiertos.
- Creado por la Organización Internacional para la Estandarización (ISO) en el año 1980





## 5. Modelos de referencia

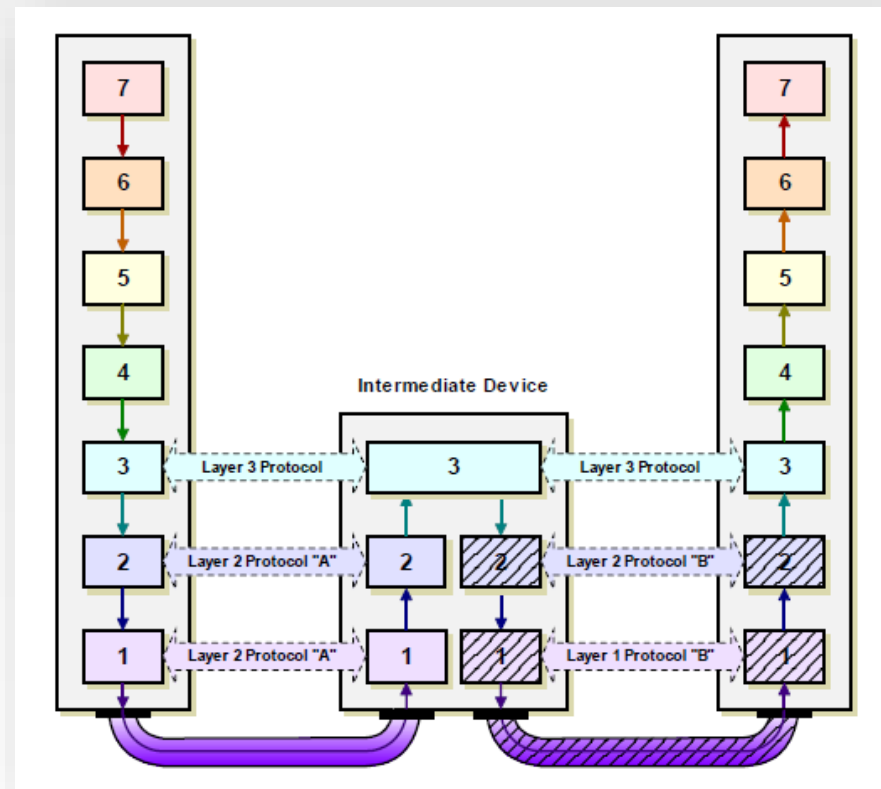
### El modelo OSI

#	Nivel	Funciones	PDU	Ámbito
1	Físico	Codificación, señalización, transmisión, recepción	Bit	Señales eléctricas/ópticas
2	Enlace	Control de Enlace Lógico, Control de Acceso al Medio	Trama	Comunicación entre extremos de un enlace
3	Red	Direccionamiento de hosts, encaminamiento, encapsulamiento, fragmentación y reensamblado, diagnóstico y manejo de errores	Paquete	Comunicación entre nodos de una red
4	Transporte	Direccionamiento de procesos	TPDU	Comunicación entre procesos
5	Sesión	Gestión de sesiones	SPDU	Sesiones entre procesos
6	Presentación	Traducción, compresión, codificación	PPDU	Datos de aplicación
7	Aplicación	Servicios	APDU	Datos de aplicación

## 5. Modelos de referencia

### El modelo OSI

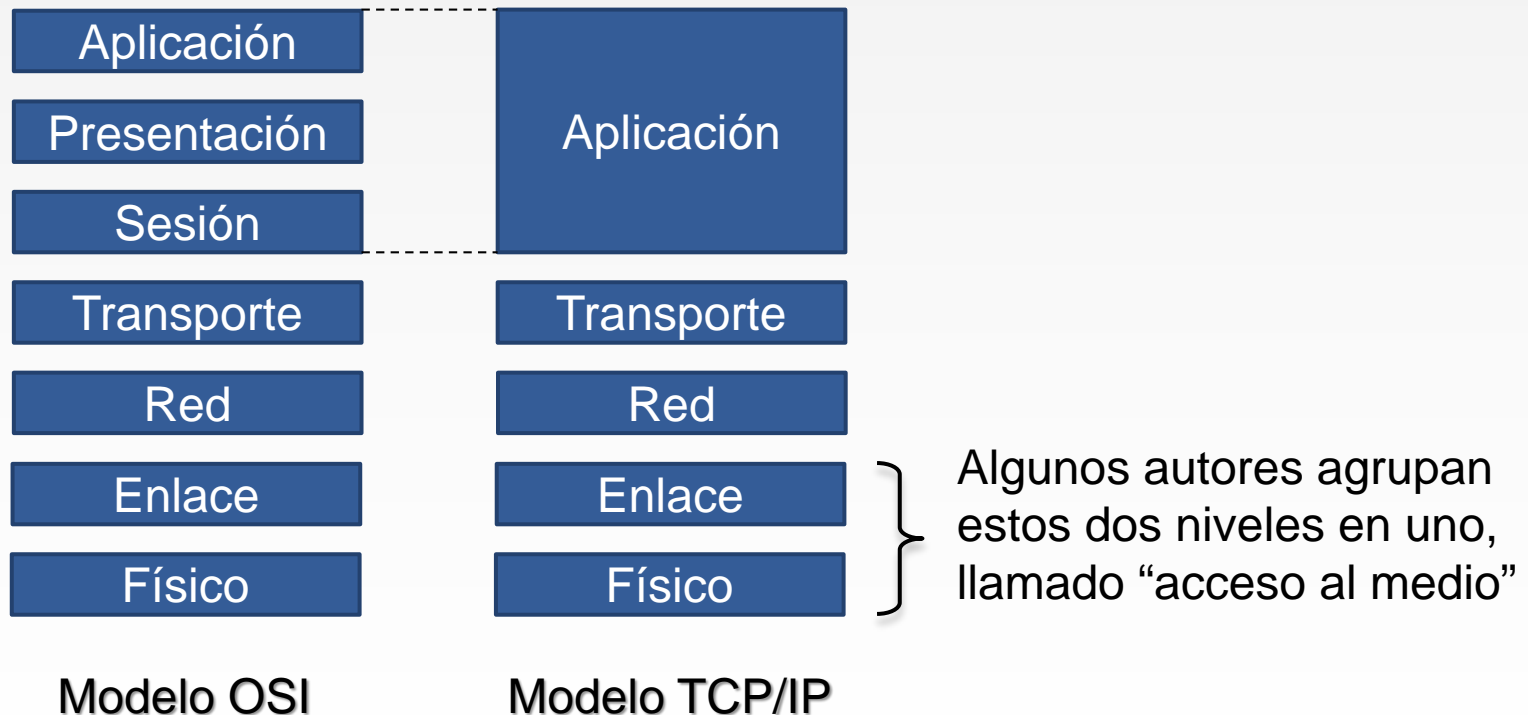
- Los equipos terminales (hosts) implementan los 7 niveles del modelo OSI
- Los nodos intermedios sólo implementan hasta el nivel 3 (red)



## 5. Modelos de referencia

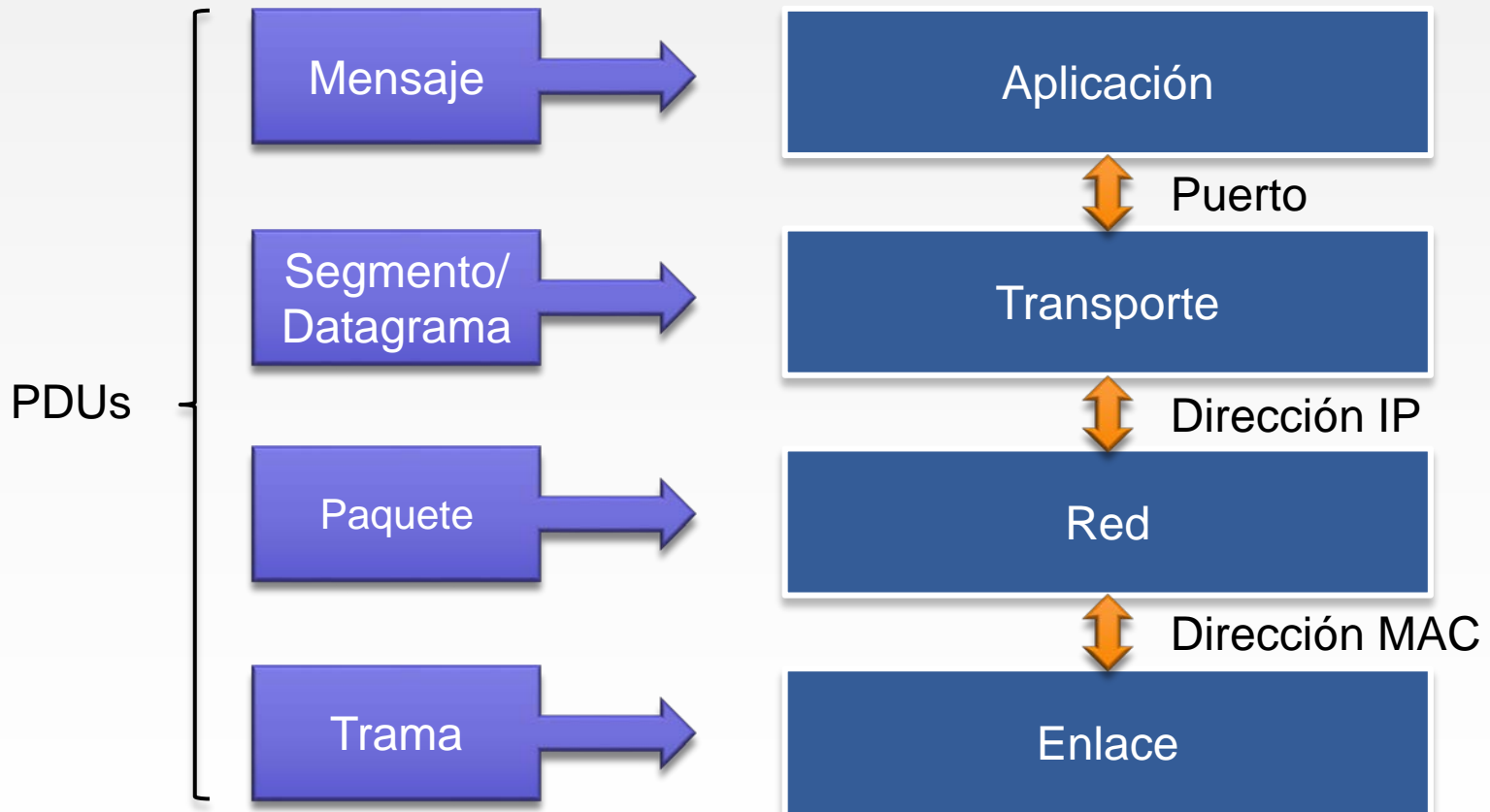
### El modelo TCP/IP

- El modelo TCP/IP tiene 5 niveles:



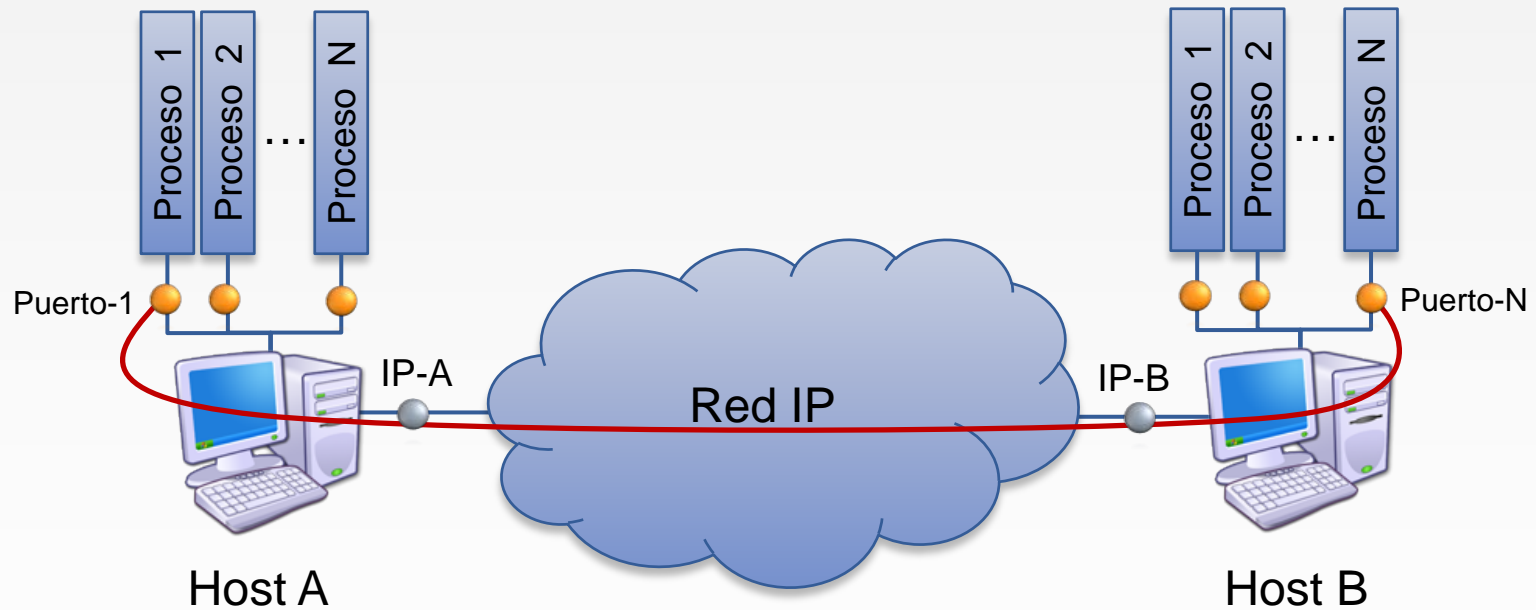
## 5. Modelos de referencia

### El modelo TCP/IP



## 5. Modelos de referencia

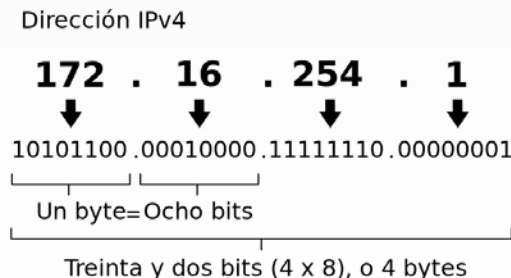
### El modelo TCP/IP



## 5. Modelos de referencia

### El modelo TCP/IP

- Dirección nivel transporte: **puertos** TCP/UDP (16 bits): [RFC 6335](#)
  - 0-1023: Puerto de sistema (*well-known ports*). Reservados para servicios distribuidos en Internet (correo electrónico, web, etc). Son usados por procesos de sistema (necesitan permisos de administrador)
  - 1024-49151: Puertos de usuario, de libre utilización
  - 49152-65535: Puertos efímeros, de uso dinámico. Se utilizan sobre todo por los clientes al conectar con servidores
- Direcciones nivel red: **direcciones IP** (32 bits):



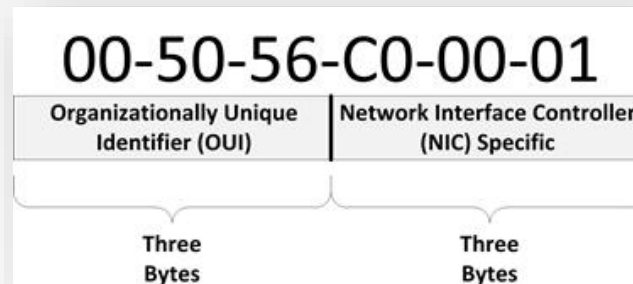
Notación decimal con puntos:  
dividimos los 32 bits en 4 y lo  
representamos en decimal

## 5. Modelos de referencia

---

### El modelo TCP/IP

- Dirección nivel enlace: **direcciones MAC** (48 bits = 8 bytes):

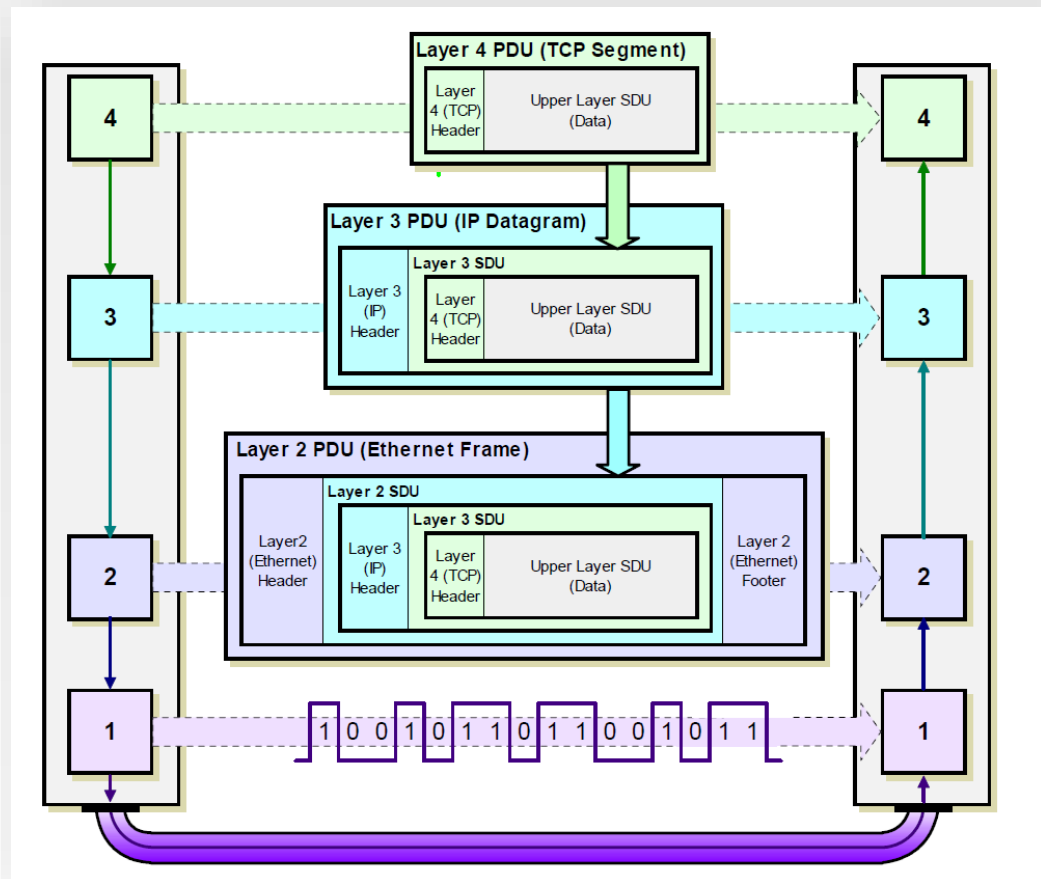


- Se conoce también como dirección física, y es única para cada dispositivo
- Las direcciones MAC están administradas por el IEEE

## 5. Modelos de referencia

### El modelo TCP/IP

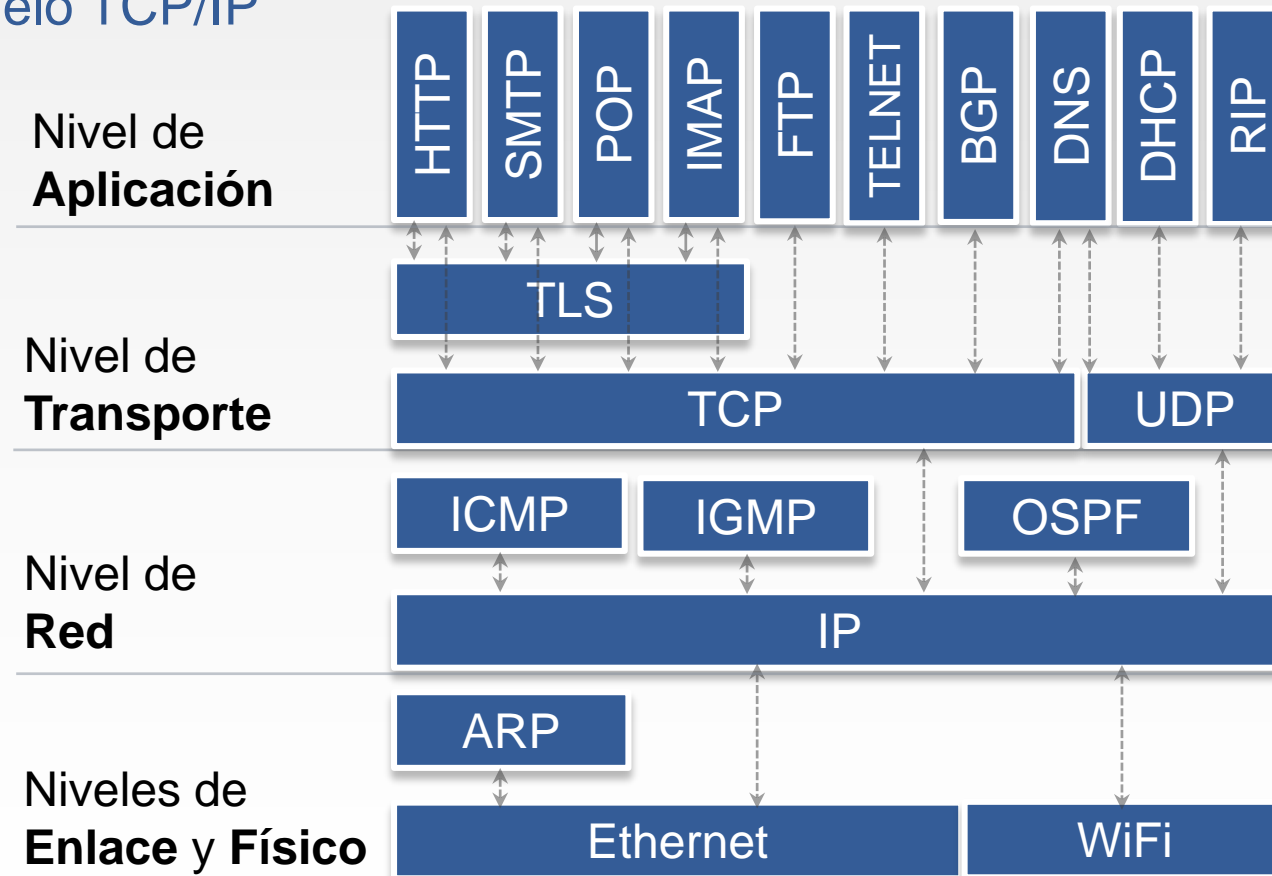
- Encapsulación de PDUs:





## 5. Modelos de referencia

### El modelo TCP/IP



# Índice de contenidos

---

1. Introducción
2. ¿Qué es Internet?
3. Un poco de historia
4. Tipos de redes
5. Modelos de referencia
6. **Análisis de protocolos**

## 6. Análisis de Protocolos

---

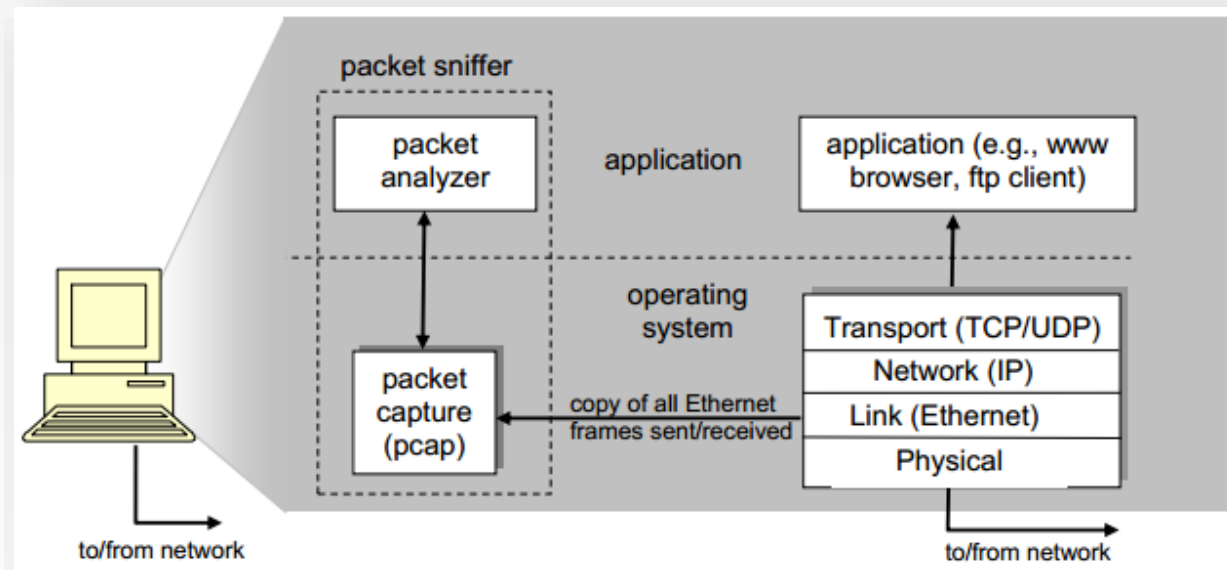
- Un analizador de protocolos (*packet sniffer*) es una herramienta que captura los paquetes enviados/recibidos en un sistema terminal
- Se dice que son sistemas pasivos ya que no permiten modificar el tráfico analizado
- Wireshark es el analizador de protocolos que vamos a usar para realizar ejercicios prácticos en la asignatura



<https://www.wireshark.org/>

## 6. Análisis de Protocolos

- Un *sniffer* tiene dos componentes:
  - Librería de captura de paquetes (`pcap`): Recibe una copia de cada trama (PDU de nivel 2) enviado o recibido por el host (equipo terminal)
  - Analizador de paquetes: Muestra por pantalla todos los datos enviados/recibidos.



# 6. Análisis de Protocolos

Menú

Filtro

Tráfico  
capturado

Detalle de  
una trama

Paquete en  
HEX y ASCII

The screenshot shows the Wireshark interface with the following components:

- Menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Filter:** Apply a display filter ... <Ctrl-/>
- Tráfico capturado (Packet List):**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	74.125.133.125	192.168.1.128	TCP	539	5222 → 49859 [PSH, ACK] Seq=1 Ack=1 Win=1185 Len=485 [TCP segment of a re...
2	0.036714	192.168.1.128	216.58.214.170	TCP	1434	61991 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1380 [TCP segment of a re...
3	0.036742	192.168.1.128	216.58.214.170	TLSv1.1	775	Application Data
4	0.050615	192.168.1.128	74.125.133.125	TCP	54	49859 → 5222 [ACK] Seq=1 Ack=486 Win=254 Len=0
5	0.143046	216.58.214.170	192.168.1.128	TCP	54	443 → 61991 [ACK] Seq=1 Ack=2102 Win=230 Len=0
6	0.272489	192.168.1.128	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
7	0.401620	216.58.214.170	192.168.1.128	TLSv1.1	539	Application Data
8	0.401623	216.58.214.170	192.168.1.128	TLSv1.1	1003	Application Data
9	0.401625	216.58.214.170	192.168.1.128	TLSv1.1	107	Application Data
10	0.401626	104.244.42.136	192.168.1.128	TLSv1.2	100	Application Data
11	0.401815	192.168.1.128	216.58.214.170	TCP	54	61991 → 443 [ACK] Seq=2102 Ack=1488 Win=258 Len=0
12	0.402142	104.244.42.136	192.168.1.128	TLSv1.2	100	Application Data
13	0.402143	216.58.214.170	192.168.1.128	TLSv1.1	107	[TCP Spurious Retransmission], Application Data
14	0.402233	192.168.1.128	216.58.214.170	TCP	66	[TCP Dup ACK 11#1] 61991 → 443 [ACK] Seq=2102 Ack=1488 Win=258 Len=0
15	0.402411	192.168.1.128	104.244.42.136	TCP	54	59180 → 443 [FIN, ACK] Seq=1 Ack=93 Win=253 Len=0
- Detalle de una trama (Packet Details):**
  - Frame 1: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface 0
  - Ethernet II, Src: Zte\_e8:12:0f (70:2e:22:e8:12:0f), Dst: LiteonTe\_7d:fb:95 (74:df:bf:7d:fb:95)
  - Internet Protocol Version 4, Src: 74.125.133.125, Dst: 192.168.1.128
  - Transmission Control Protocol, Src Port: 5222, Dst Port: 49859, Seq: 1, Ack: 1, Len: 485
- Paquete en HEX y ASCII:**

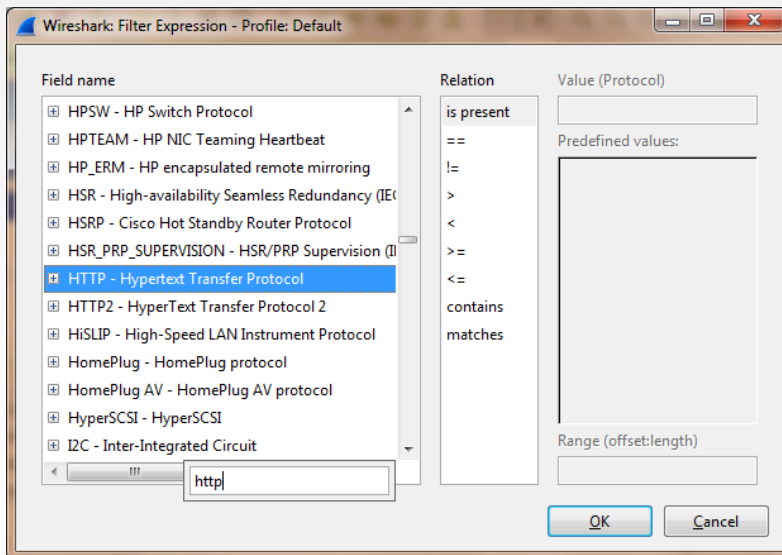
```

0000  74 df bf 7d fb 95 70 2e 22 e8 12 0f 08 00 45 00  t...p. ....E.
0010  02 0d 68 fa 00 00 30 06 8d ce 4a 7d 85 7d c0 a8  ..h..0. ..}]...
0020  01 80 14 66 c2 c3 5f a4 71 bb c5 78 d7 8f 50 18  ...f... q..x..P.
0030  04 a1 3c 03 00 00 17 03 02 01 e0 77 38 32 7c f2  <..... w02].
0040  d1 5e ab 17 c0 53 c7 39 db c1 a6 55 b9 89 6f a3  ^...S.9 ..U..o.
0050  11 72 5d d5 bd 23 8d 4a f5 3a 46 74 1d 86 79 60  .r]..#J .:Ft..y'
0060  74 f7 c2 90 22 43 eb 2c b0 6b 68 3f 5c 18 b9 0e  t...C,. .kh?{\...
0070  9d cd 09 88 f9 73 43 d5 df 41 46 b4 44 a6 4c 2d  ....sC. .AF.D.L
0080  08 46 3a 92 df 7d 32 aa 3d f7 63 43 81 4e 4e a8  .F:..}2. =.cC.NN.
0090  9d 69 f6 58 99 8e ab de 24 00 65 5a 6c d2 c2 c0  .i.X... $.eZL...
00a0  b2 fb b0 8a 2a 09 35 1f 27 1b ca 62 d4 35 2c b8  ...*.5. '.b.5..
00b0  df 83 a2 29 f8 57 9a 5c ac b6 cb 18 0a ce 7b 35  (...).W.\ .....{5
00c0  b1 a1 6e 5e 04 6e b1 53 c9 a3 c6 9d 96 79 f9 0a  ..n^n.S .....y..
00d0  85 05 2f 29 6f f6 b2 fb 86 34 21 3f 22 61 f7 ae  ../)o... .4!?"a.
00e0  a0 b3 16 53 88 2d e0 0b dd d7 7e 69 4e 81 80 8b  ..S... ..iN...
00f0  6b fa eb d3 d4 49 45 dc 38 6a 73 d1 b7 d9 c0 16  k...IE. 8js.....
0100  60 8c 4b 41 2e 37 b2 3d e3 dc ff 05 41 9f 0b bb  ^..KA.7= ....A...

```

## 6. Análisis de Protocolos

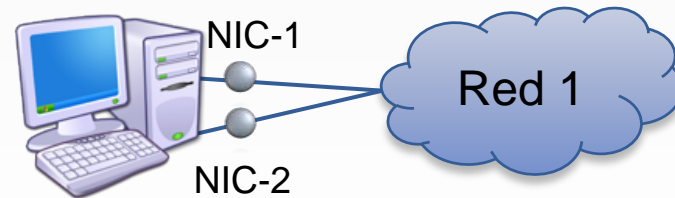
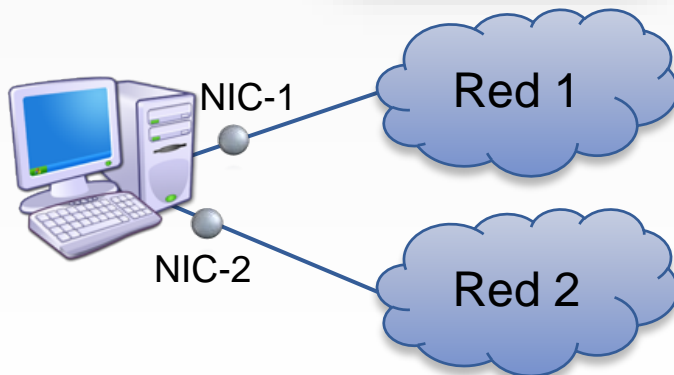
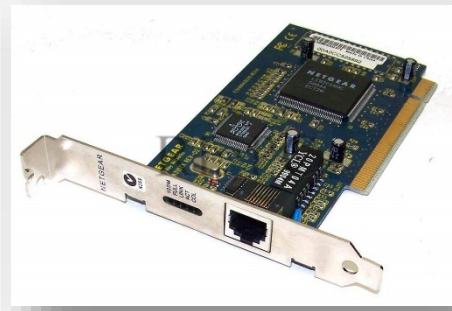
### ■ Filtrado en Wireshark



English	C-like	Description and example
eq	==	Equal. <code>ip.src==10.0.0.5</code>
ne	!=	Not equal. <code>ip.src!=10.0.0.5</code>
gt	>	Greater than. <code>frame.len &gt; 10</code>
lt	<	Less than. <code>frame.len &lt; 128</code>
ge	>=	Greater than or equal to. <code>frame.len ge 0x100</code>
le	<=	Less than or equal to. <code>frame.len &lt;= 0x20</code>

## 6. Análisis de Protocolos

- La conexión de un host a una red se realiza mediante un dispositivo (físico o virtual) llamado **interfaz de red** (*Network Interface Card, NIC*)



## 6. Análisis de Protocolos

---

- En sistemas UNIX/Linux, además de los interfaces de red (virtuales o físicos) de un host, existe un interfaz virtual llamado interfaz de *loopback*
- Es un interfaz que simula la conexión de un host consigo mismo (*localhost*)
- En sistemas Windows no existe este concepto, con lo que para capturar el tráfico de la interfaz local se necesitará una herramienta externa como [RawCap](#)
- Para capturar todo el tráfico de una red Wifi es necesario que la tarjeta de red soporte captura en modo promiscuo (capturar tramas emitidas o dirigidas a otros dispositivos)