Escuela de
Ingeniería y Arquitectura
Universidad Zaragoza

Departamento de
Informática e Ingeniería
de Sistemas
Universidad Zaragoza



Tema 1: Servicios de Red

Garantía y Seguridad (30242)

4º curso, Grado en Ingeniería Informática

especialidad en

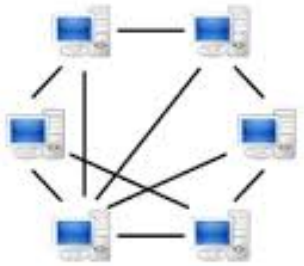
Ingeniería de Computadores

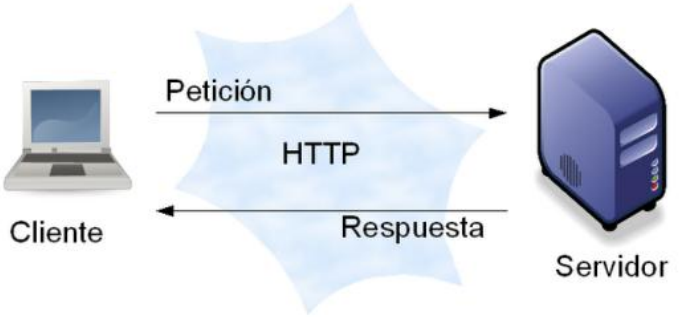
J. Alastruey, P. Ibáñez, D. Suárez, V. Viñals
Área de Arquitectura y Tecnología de Computadores (ATC)

1. Servicio de red

- Servicio:
  - DRAE: 7. Favor que se hace a alguien

- Servicio de red
  - Ofrecido por
    - Servidor
    - Par, igual (peer)





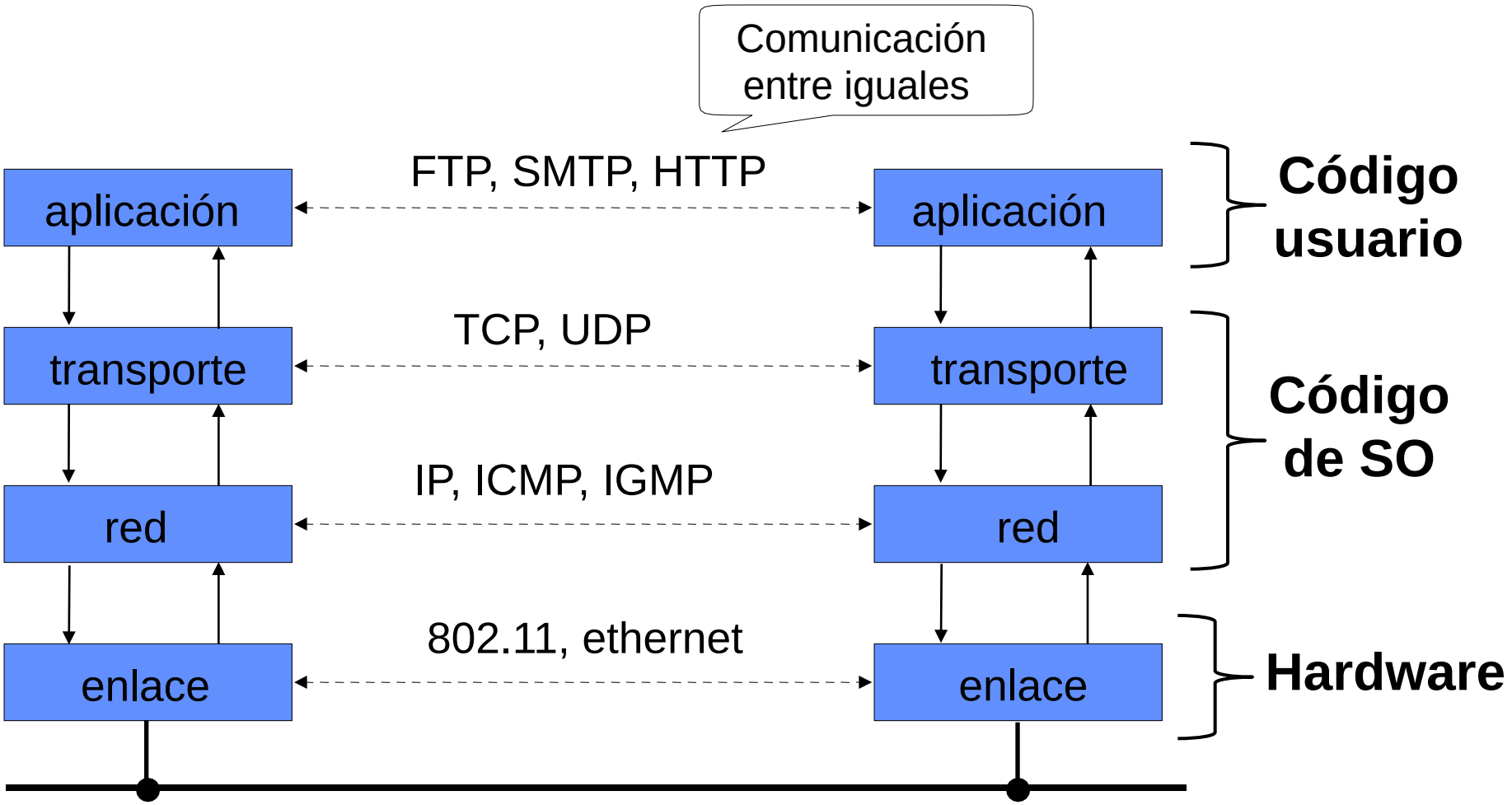
- Proceso (demonio) ejecutándose en un servidor
  - Servicio de tiempo: NTP
  - Servicio de nombres: DNS
  - Servicio de correo: SMTP, IMAP
  - Servicio HTTP

Índice del tema

- Repaso de TCP/IP
- Internet: gestión y administración

1. TCP / IP

- Pila de protocolos TCP/IP



1. TCP / IP

- Encapsulamiento TCP/IP

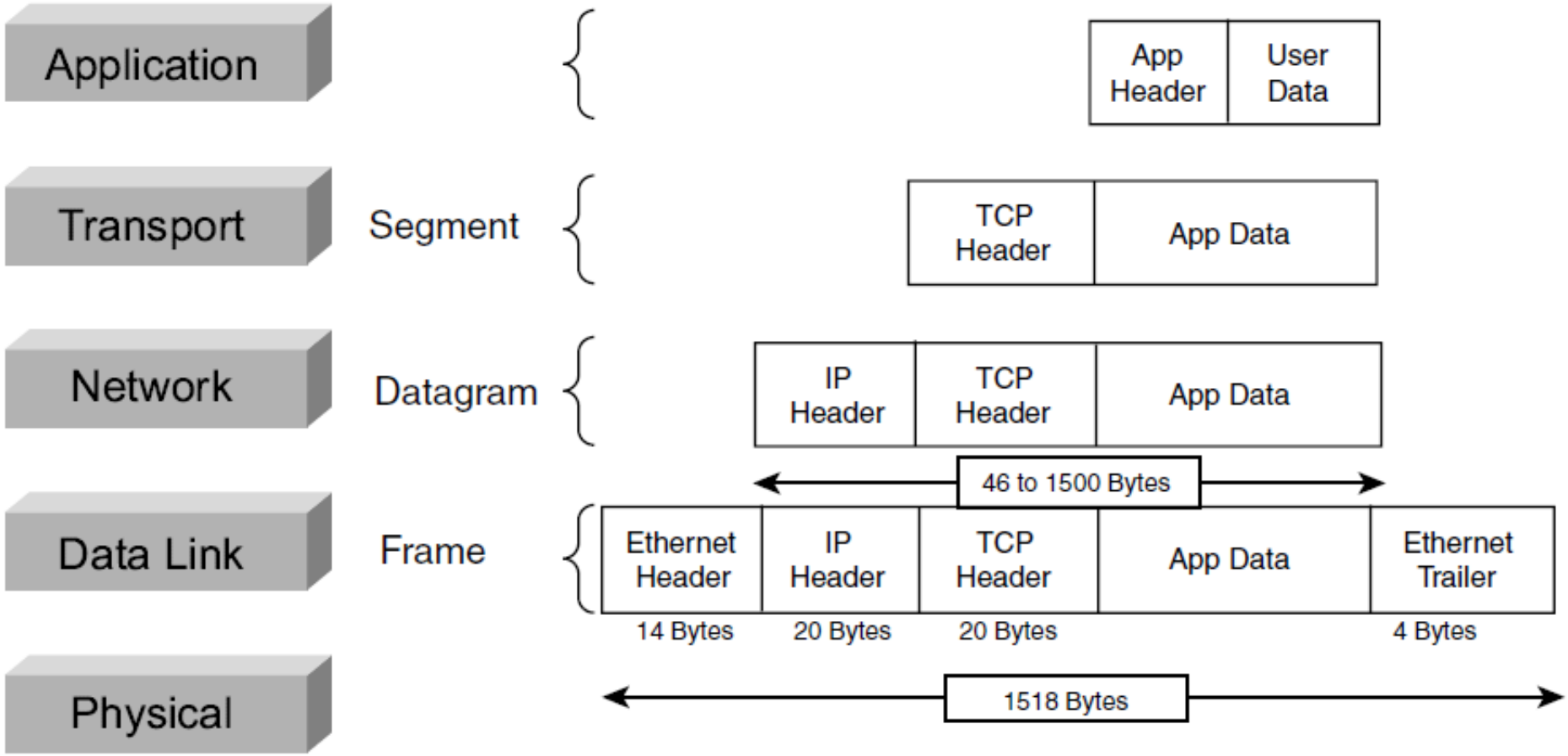


Figura: Data Center Fundamentals

1. Nivel de transporte: TCP

- TCP: Transmission Control Protocol
  - RFC 793 y otros posteriores
- Entrega fiable de flujo extremo a extremo
  - Permite la recuperación de
    - paquetes perdidos, erróneos, desordenados, duplicados
  - Mecanismos
    - Número secuencia (SEQ), código control, confirmación recepción (*ACK*), temporizadores espera + retransmisión
- Control de flujo
  - Regulación de velocidad entre los extremos de la comunicación
  - El receptor no debe desbordarse
- Control de congestión
  - Mantenimiento del número de paquetes en la red por debajo de un nivel a partir del cual se degradan sus prestaciones

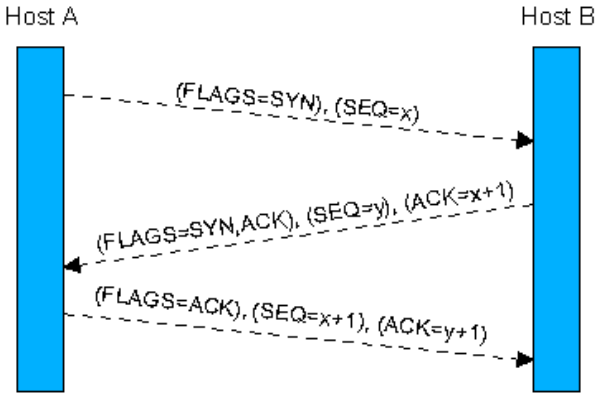
1. Nivel de transporte: TCP

- Permite la **multiplexación**
  - Distintos procesos en una máquina: puertos

- Puertos TCP (16 bits)
  - Puntos abstractos de origen o destino utilizados por los procesos
  - Fichero `/etc/services`
  - Asignados por IANA
    - http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml
  - Puertos “bien conocidos”: 0-1023
    - FTP: 20, 21, Telnet: 23, SMTP: 25, HTTP: 80
    - Privilegiados: sólo procesos con permisos de administrador
  - Puertos registrados: 1024-49151
  - Puertos dinámicos o privados: 49152-65535

1. Nivel de transporte: TCP

- Servicio orientado a conexión extremo a extremo
  - Establecimiento de conexión
  - Transferencia de datos
  - Liberación de conexión



- Conexión definida por 2 puntos extremos (= 2 sockets)
- socket = < dirección IP + nº puerto >
  - Puede ser compartido por varias conexiones
    - Servidor web: <@ IP, 80>

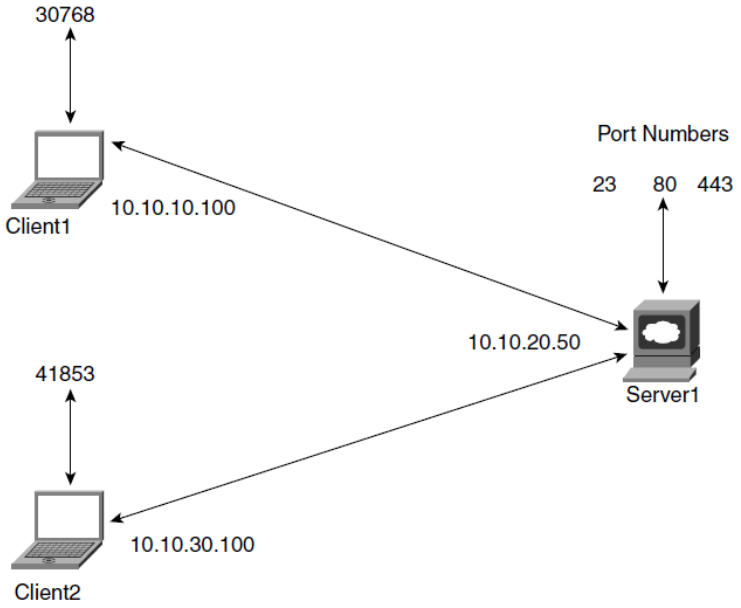
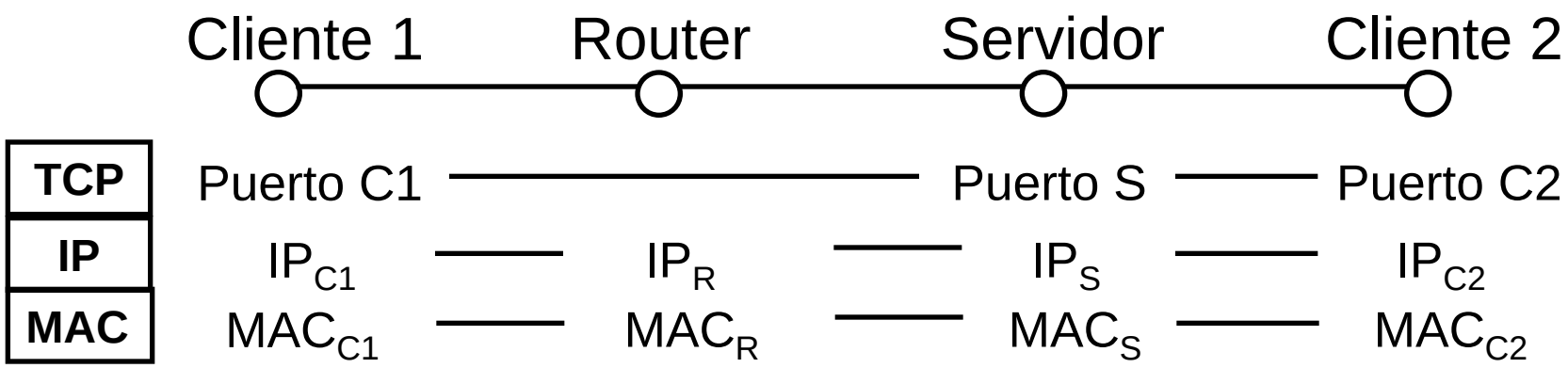


Figura superior:
http://www.rvs.uni-bielefeld.de/~heiko/tcpip/tcpip_html_alt/kap_2_4.html#tcp
Figura inferior: Data Center Fundamentals, página 259

1. Nivel de transporte: TCP

- Detalla las conexiones existentes



Conexión 1: <IP_{C1}, puerto C1> + <IP_S, puerto S>
Conexión 2: <IP_{C2}, puerto C2> + <IP_S, puerto S>

1. Nivel de transporte: UDP

- UDP:User Datagram Protocol
  - RFC 768: Fundamentos de UDP
- Servicio no fiable, no orientado a conexión
  - (opcional) Garantiza la integridad de los datos (*checksum*)

- Puertos UDP (16 bits)
  - Identifican el proceso al que se asocian los datos
  - Distintos de los puertos TCP
  - Puertos “conocidos” (p. ej. TFTP: 69, DNS: 53, SNMP: 161)
  - Puertos privilegiados (<1024)

1. Nivel de transporte: otros protocolos

- QUIC
  - RFC 9000
  - Web (HTTP/3), baja latencia
  - Transporte fiable sobre UDP
- SCTP
  - RFC 4960
  - Telefonía IP, aplicaciones multimedia

1. Nivel de transporte

- Sockets C: interacción cliente – servidor

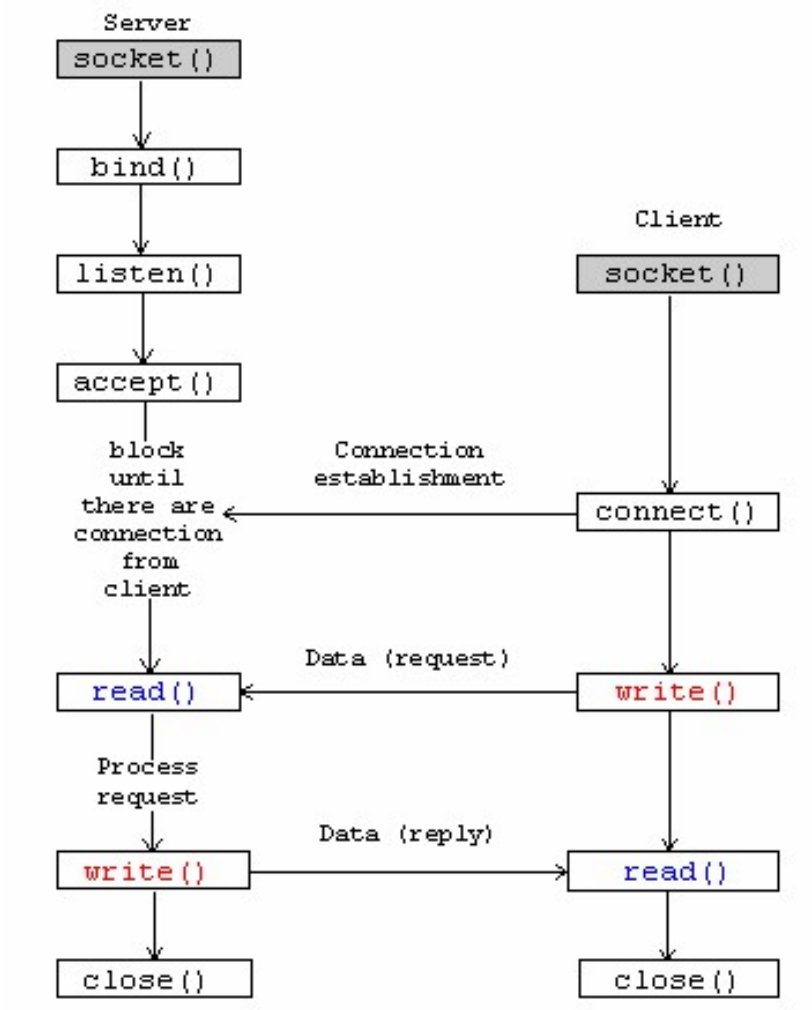


Figura: https://stackoverflow.com/questions/27014955/socket-connect-vs-bind

1. Nivel de transporte

- Sockets C: código

Servidor

```
sock_fd = socket(AF_INET, SOCK_STREAM, 0);
memset(&sa, 0, sizeof sa);
sa.sin_family = AF_INET;
sa.sin_addr.s_addr = INADDR_ANY;
sa.sin_port = listen_port;
n = bind(sock_fd , (struct sockaddr *) &sa, sizeof(sa));
rc = listen(listen_s, LISTEN_QUEUE);
rc = accept(listen_s, (struct sockaddr *)&sa, sizeof(sa));
```

Cliente

```
sock_fd = socket(AF_INET, SOCK_STREAM, 0);
memset(&sa, 0, sizeof sa);
sa.sin_family = AF_INET;
inet_pton(AF_INET, ip, &sa.sin_addr)
sa.sin_port = htons(port);
rc = connect(client_s, (struct sockaddr *)&sa, sizeof sa);
```

1. Nivel de transporte

- Socket cliente bash

Cliente

```
bash$ exec 5<>/dev/tcp/webdiis.unizar.es/80
bash$ echo -e "GET / HTTP/1.0\n" >&5
bash$ cat <&5
HTTP/1.1 200 OK
[...]
Content-Type: text/html

<HTML>
<HEAD><TITLE>webdiis.unizar.es</TITLE></HEAD>
<BODY BGCOLOR="#FFFFFF" TEXT="#000000">
<H1 ALIGN=CENTER>webdiis.unizar.es</H1>
<P>Este es el servidor web secundario del DIIS del CPS.</P>
</BODY>
</HTML>
```

Referencia: https://tldp.org/LDP/abs/html/devref1.html

1. Nivel de transporte

- Identificación de servicios de red en estado de escucha y proceso asociado

```
lab000:~/ ss -lpt
State  Recv-Q Send-Q   Local Address:Port             Peer Address:Port Process
[…]
LISTEN 0      128            0.0.0.0:ssh                   0.0.0.0:*
lab000:~/ ss -lpu
[…]
```

- Monitorización del estado de las conexiones

```
lab000:~/ ss -a
Netid   State        Recv-Q   Send-Q     Local Address:Port     Peer Address:Port        Process
[…]
tcp     LISTEN       0        128        0.0.0.0:ssh            0.0.0.0:*
tcp     CLOSE-WAIT   1        0          155.210.152.177:36660  35.186.224.24:https
tcp     ESTAB        0        0          127.0.0.1:33501        127.0.0.1:36602
tcp     ESTAB        0        0          155.210.152.177:ssh    10.1.165.144:64153
tcp     ESTAB        0        0          127.0.0.1:36602        127.0.0.1:33501
tcp     ESTAB        0        0          155.210.152.177:34992  155.210.152.183:ldap
tcp     ESTAB        0        0          155.210.152.177:ssh    155.210.139.121:61626
tcp     CLOSE-WAIT   1        0          155.210.152.177:36656  35.186.224.24:https
tcp     CLOSE-WAIT   1        0          155.210.152.177:51918  98.86.250.202:https
```

1. Nivel de transporte

- netcat: cliente/servidor TCP/UDP
  - Herramienta depuración

```
linux$ echo -e "HEAD / HTTP/1.0\n" | nc  webdiis.unizar.es 80
HTTP/1.1 200 OK
Date: Wed, 25 Mar 2015 22:18:24 GMT
Server: Apache/2.2.25
Last-Modified: Tue, 04 Jun 2013 12:03:13 GMT
ETag: "174f16-6a2-4de52dd963030"
Accept-Ranges: bytes
Content-Length: 1698
Connection: close
Content-Type: text/html
```

```
linux$ man echo
[…]
 -e     enable interpretation of backslash escapes
[…]
```

1. Identificación de SO por pila TCP/IP

- TCP/IP *fingerprinting*
- Pasivo
  - Análisis de paquetes
    - Tamaño de Ventana
    - TTL (Time To Live - Tiempo de Vida)
    - DF - bit Don't Fragment
    - TOS - Type of Service
  - Difícil de detectar, poco preciso

1. Identificación de SO por pila TCP/IP

Sistema Operativo	Versión	Plataforma	TTL	WINDOW	DF	TOS
Linux	5.x–6.x	x86_64/ARM	64	29200–65535	y	0
Windows	10/11	x86_64	128	64240–65535	y	0
macOS	12–14	ARM/x86_64	64	65535	y	0
FreeBSD	12–14	x86_64	64	65535	y	0
OpenBSD	7.x	x86_64	64	16384–65535	y	0
iOS	16–17	ARM	64	65535	y	0
Android	10–14	ARM	64	5720–65535	y	0
Cisco IOS	15.x	Network HW	255	4128–65535	y	0
JunOS	20.x	Network HW	64	65535	y	0
Windows Server	2019–2022	x86_64	128	64240–65535	y	0
Docker/Linux	5.x kernel	container	64	igual host	y	0

1. Identificación de SO por pila TCP/IP

- Activo
  - Cada SO responde de forma distinta a paquetes mal formados
  - Más preciso, detectable
  - nmap

```
$ sudo nmap -O lab000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-04-08 10:15 CEST
[…]
MAC Address: 00:25:90:FC:2E:78 (Super Micro Computer)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

2. Internet: Historia, Administración

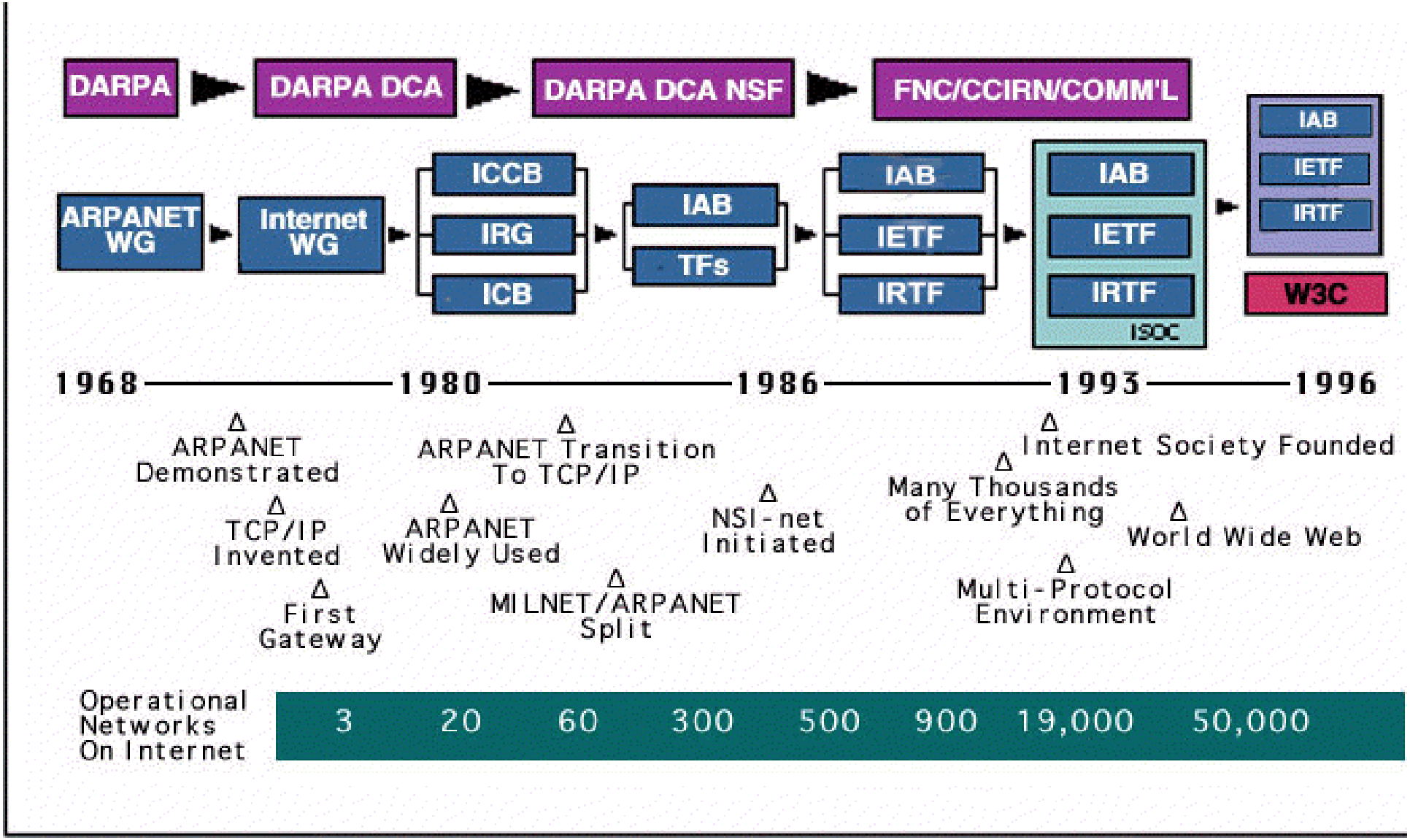


Figura: https://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

2. Internet: Administración

- Gestión de Internet necesaria para
  - Homogeneizar y evitar el aislamiento de redes = **interoperabilidad**
- Gestión
  - Administrativa, Técnica, Política
- Organismos principales
  - Internet Corporation for Assigned Names and Numbers
    - Asignación de direcciones, dominios, nº puertos …
  - Internet Society (ISOC)
    - Representa a los usuarios de Internet
    - Padre del **Internet Engineering Task Force (IETF)**
  - Internet Governance Forum (IGF)
    - Creado por la ONU en 2006
  - World Wide Web Consortium (W3C)
    - Estándares para la web

2. ISOC - Internet Society

- Organización no gubernamental y sin ánimo de lucro
- Fundada en 1992
  - https://www.internetsociety.org/history
  - https://www.wiwiw.org/pioneers/
- Mantenimiento y mejora de Internet
- Miembros organizados en “capítulos”
- Desarrolla nuevos estándares y protocolos a través de sus comités
  - IAB, IETF, IESG, IRTF, IRSG

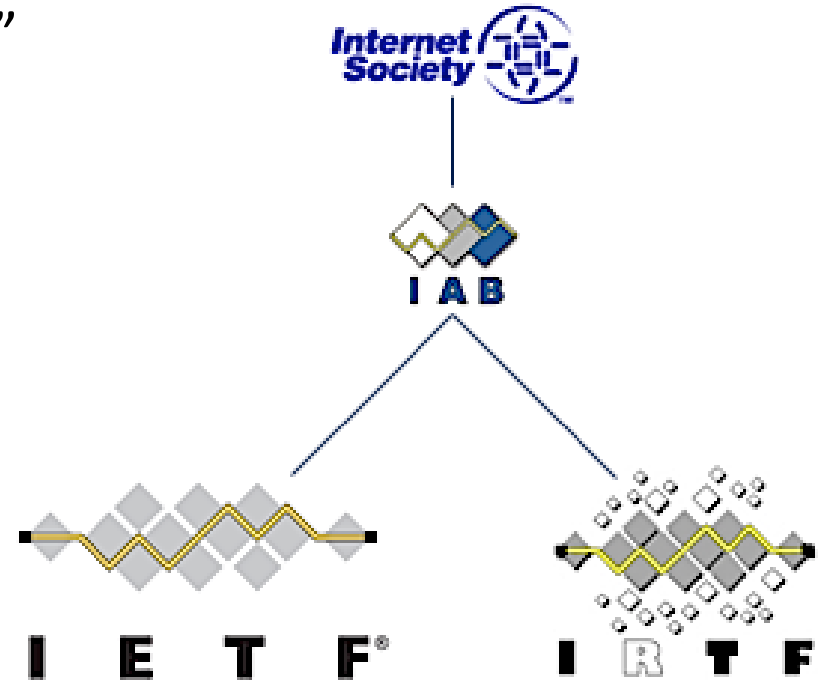


Figura: http://www.metamorphosite.com/who-owns-internet-how-it-works-domain-registration

2. ISOC - Internet Society

- IAB: Internet Architecture Board
- IETF: Internet Engineering Task Force
  - Evolución de arquitectura de Internet y su funcionamiento
  - “Comunidad abierta de diseñadores de red, operadores, fabricantes e investigadores y cualquier interesado”
  - Documentación "oficial": **RFCs**
- IESG: Internet Engineering Steering Group
  - Dirección técnica del IETF
- IRTF: Internet Research Task Force
  - Investigación para la evolución de Internet
- IRSG: Internet Research Steering Group
  - Dirección del IRTF

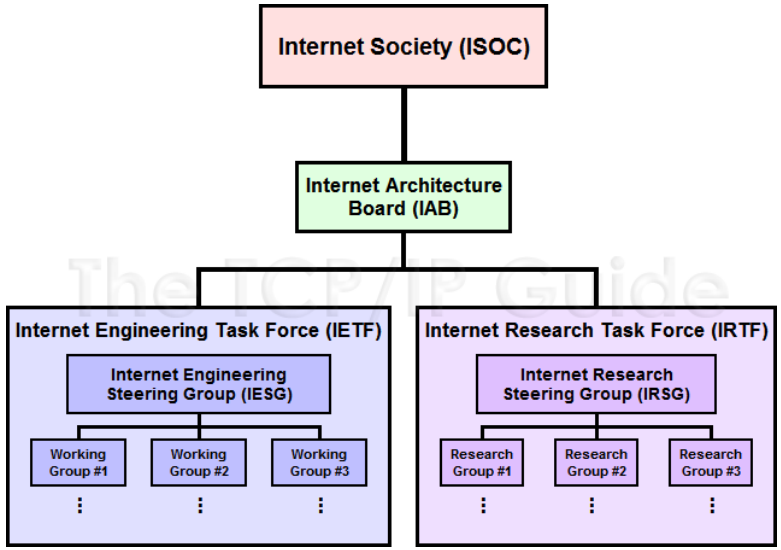


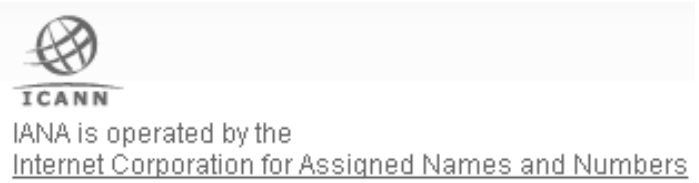
Figura: http://www.tcpipguide.com/free/t_InternetStandardsOrganizationsISOCIABIESGIETFIRSGI.htm

2. RFCs: Requests For Comments

- Base documentación técnica Internet
- Categorías (status)
  - Standards Track: protocolos
    - STD – RFC 2026
    - Fases: Proposed Standard (nº RFC asignado) ⇒ Draft Standard ⇒ Internet Standard (nº STD asignado)
  - Internet Best Current Practices: recomendaciones
    - BCP - RFC 1818
  - Informational
    - For Your Information Documents (FYI) - RFC 1150
  - Experimental
  - Historic: antiguos estándares
- Todos comienzan como Internet Drafts
- Una vez emitidos no cambian
- https://www.rfc-editor.org/search/rfc_search.php

2. IANA

- Autoridad de números Asignados de Internet
  - http://www.iana.org
- Asignación de valores para protocolos Internet
  - Gestión de la zona raíz DNS
    - Dominios de primer nivel (Top Level Domains)
    - https://www.iana.org/domains
  - Asignación de direcciones IP e identificadores AS
    - https://www.iana.org/numbers
  - Códigos y números asociados a protocolos
    - https://www.iana.org/protocols
    - Por ejemplo, telnet - puerto 23
- Funciones
  - https://www.icann.org/es/system/files/files/iana-functions-18dec15-es.pdf
  - Desempeñadas por ICANN



2. ICANN

- Internet Corporation for Assigned Names and Numbers
- Identificadores únicos (nombres de dominio e IPs)
- Gestión DNS
  - Registros: listas de dominios
  - Registradores: venta de dominios
  - Servidores raíz: almacenan lista que asocia una dirección a cada dominio del nivel principal
- Coordina asignación de direcciones IP
  - AFRINIC: África
  - APNIC: Asia Pacífico
  - ARIN: Norteamérica
  - LACNIC: Latinoamérica + Caribe
  - RIPE NCC: Europa + Oriente Medio + parte de Asia Central

Top Level Domains
Genéricos (gTLD):
.com, .net, .edu, .org
Códigos países
(ccTLD): .es, .fr, .it,

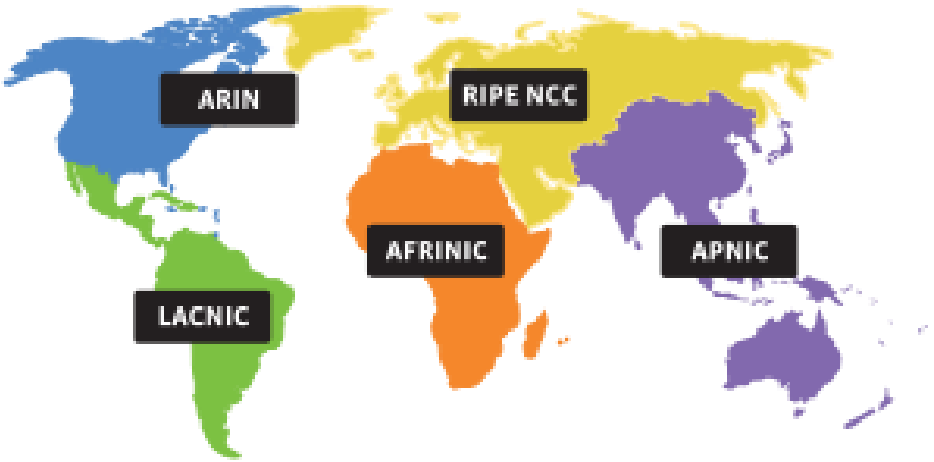


Figura: http://www.iana.org/numbers

2. W3C

- Consorcio World Wide Web (World Wide Web Consortium)
  - https://www.w3.org
- Investiga, propone y define temas y protocolos web
- Referencia y coordinación en evolución e interoperabilidad del Web
- Produce
  - Especificaciones
  - Código de referencia
  - Prototipos demostración
  - Por ejemplo,

