Seguridad de la Información

Una introducción con enfoque práctico

Ing. Mariano Aliaga

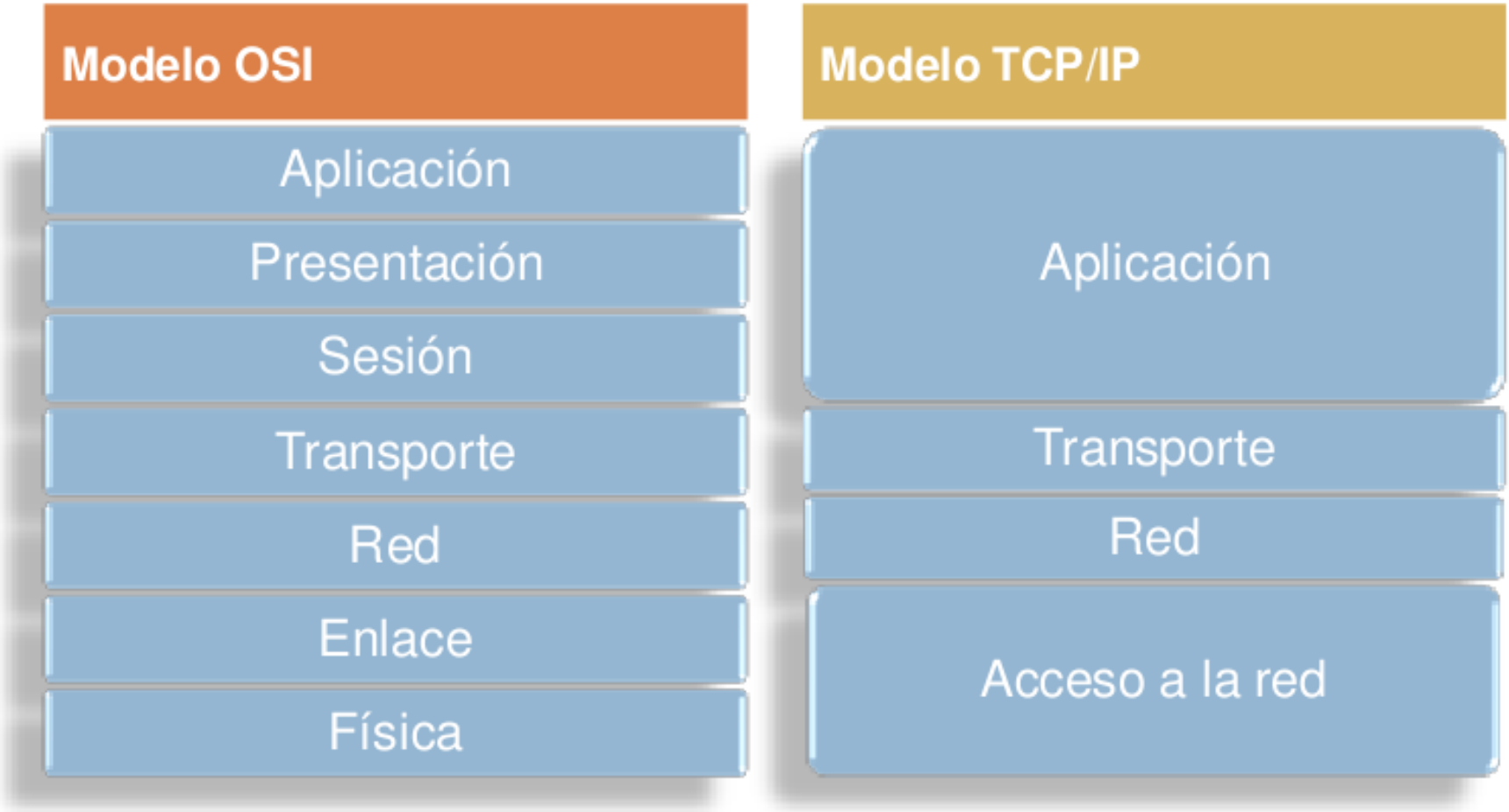
Universidad Católica de Córdoba - Facultad de Ingeniería

2021

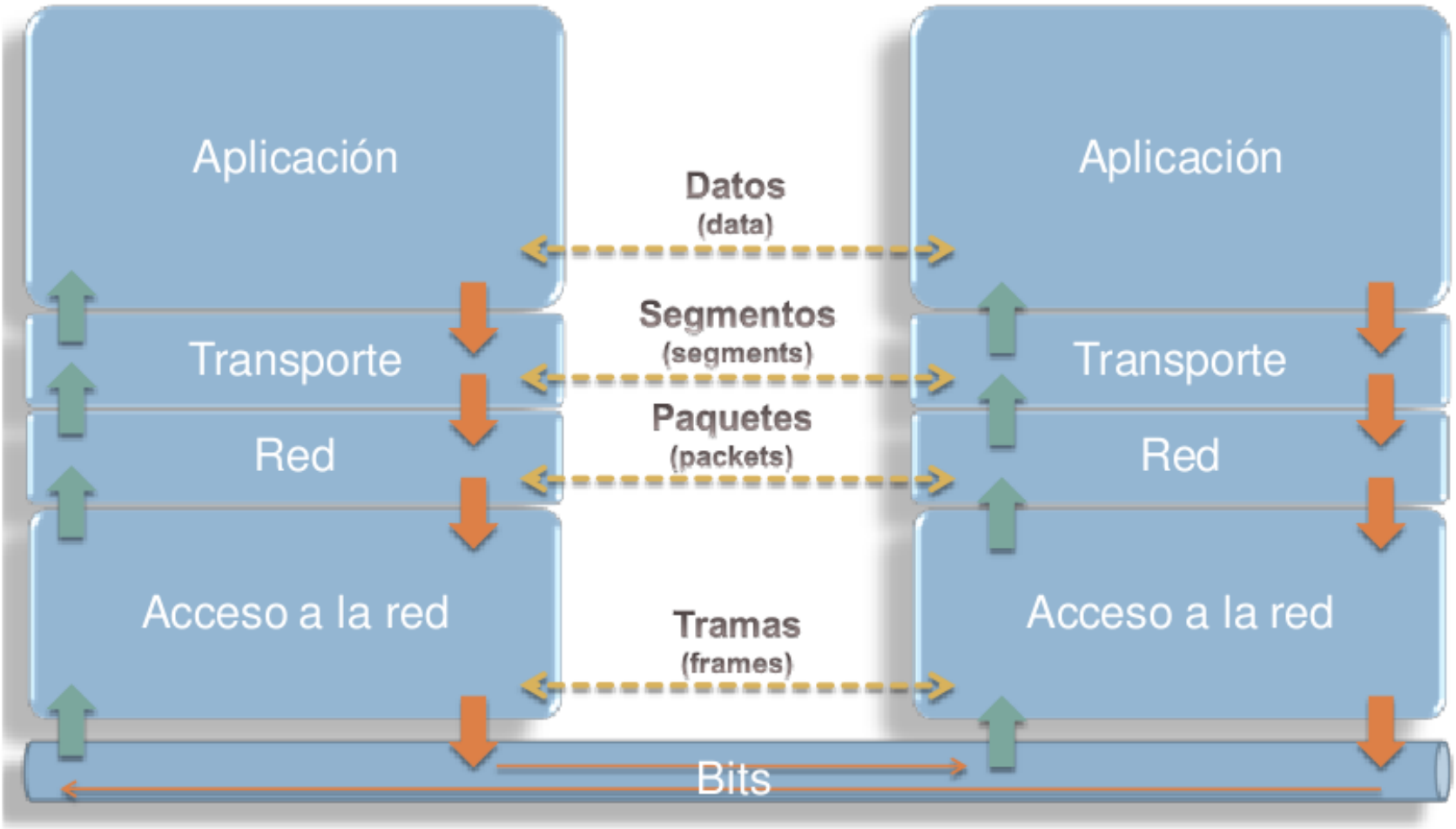
Panorama General

1. Modelo TCP/IP
   - Suite de Protocolos de Internet
   - Nivel de Acceso a la Red
   - Nivel de Red
   - Nivel de Transporte
   - Nivel de Aplicación

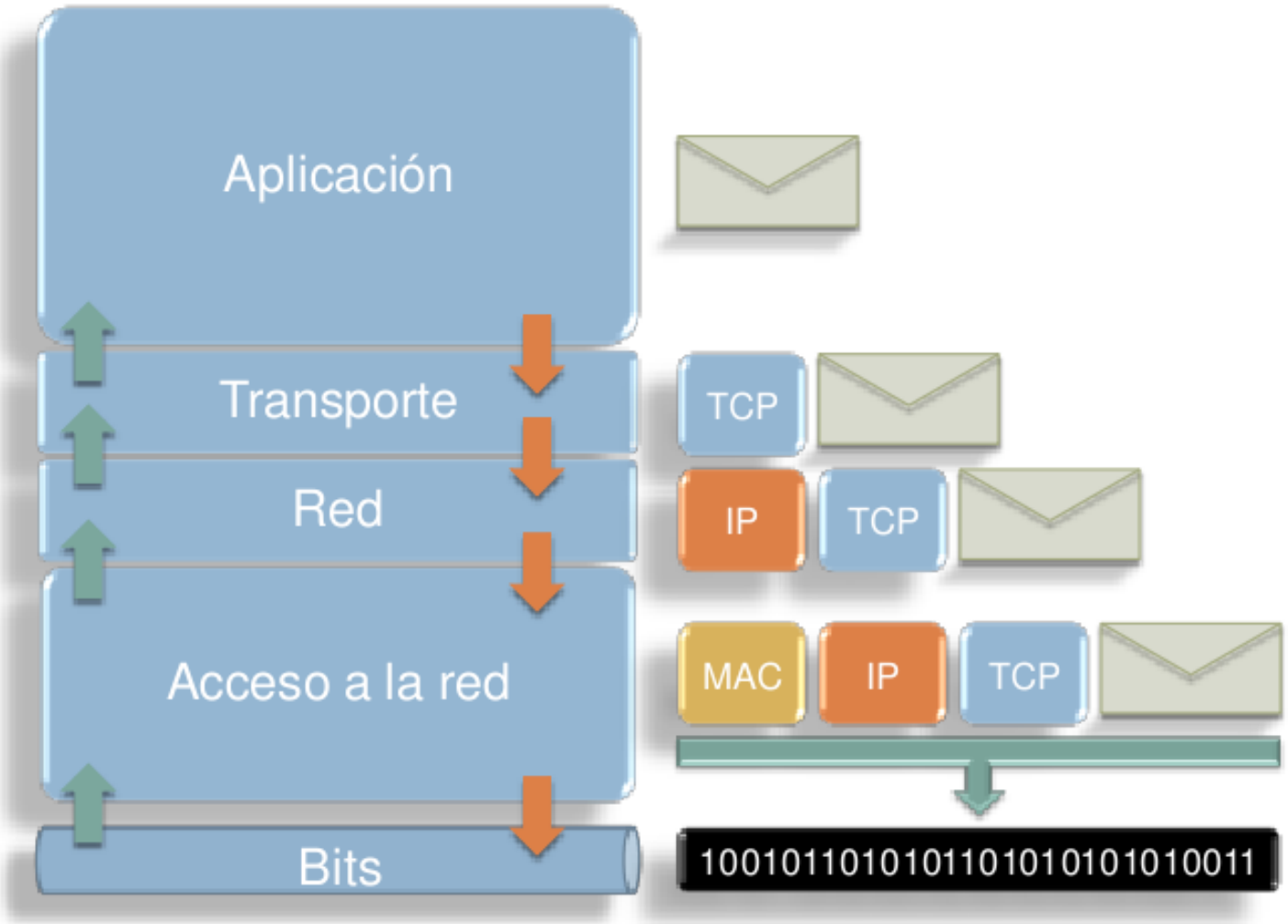
Comparación OSI y TCP/IP



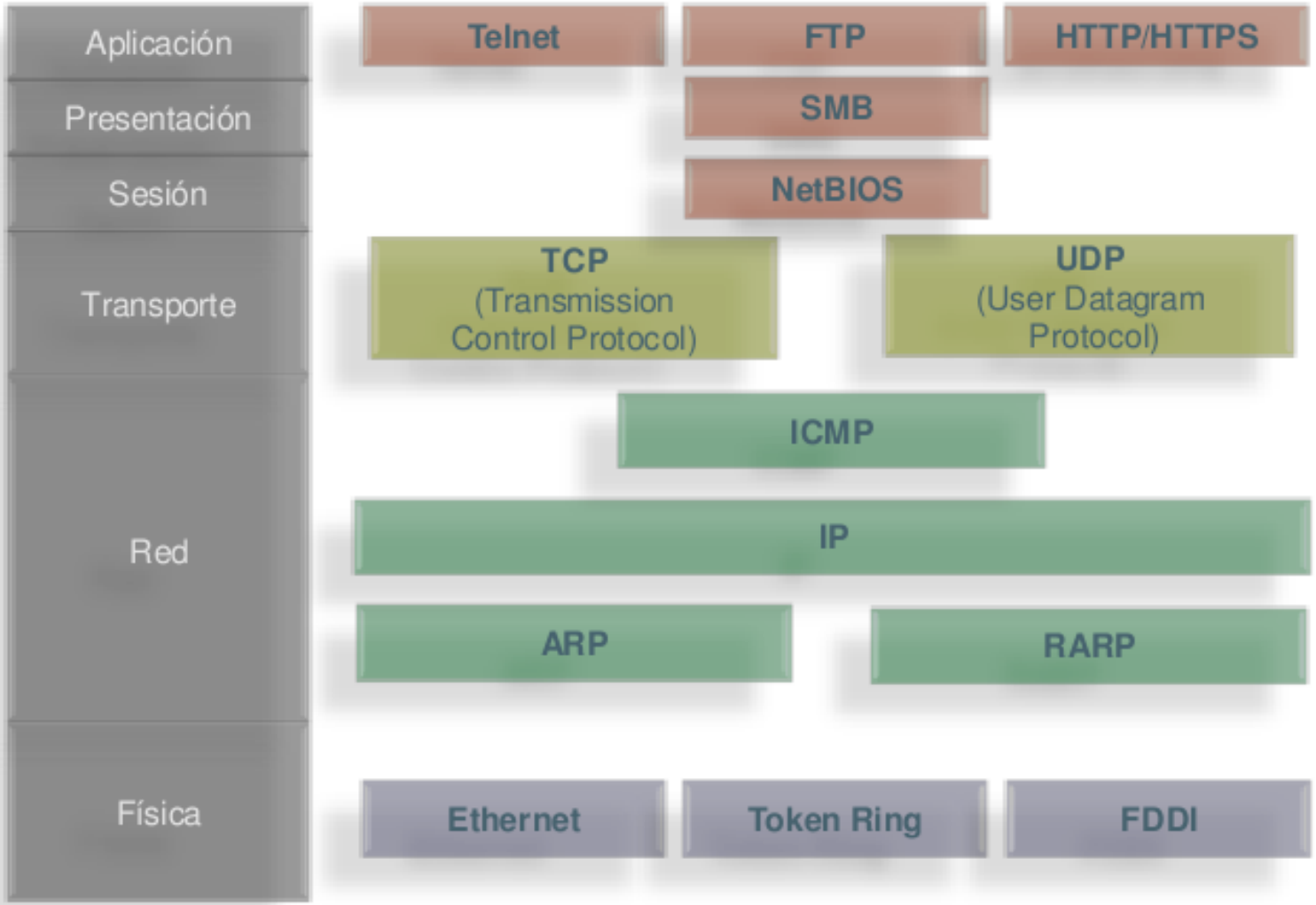
Transmisión de datos



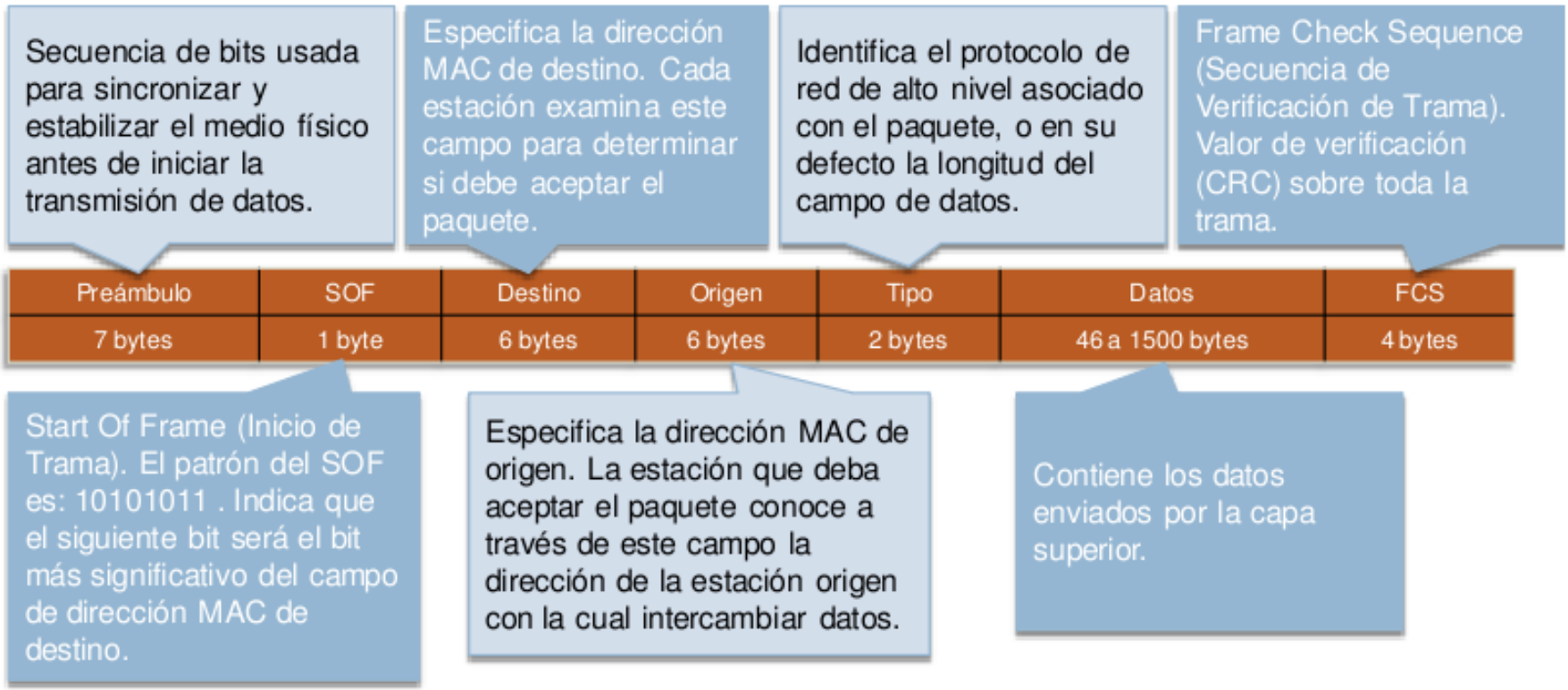
Encapsulamiento



Protocolos TCP/IP



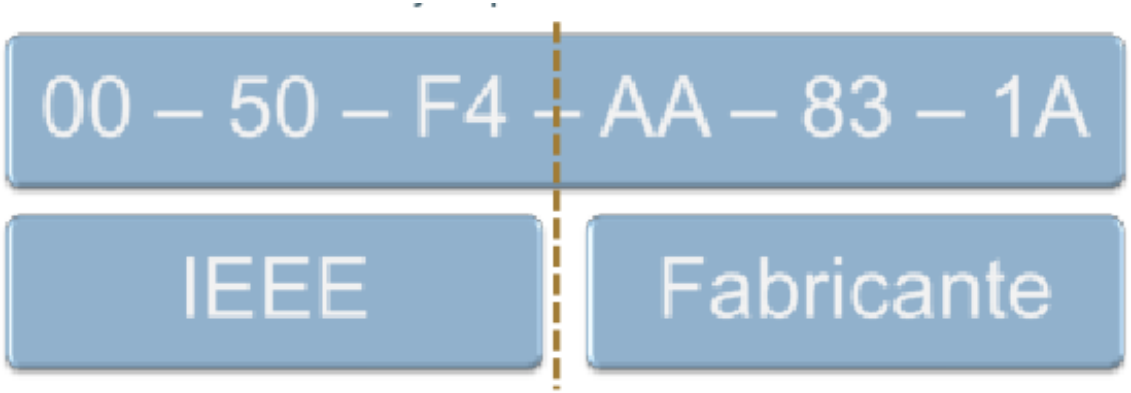
Trama Ethernet



Direccionamiento MAC

MAC (Medium Access Control): proporciona un identificador único asignado a las placas adaptadoras de red por parte del fabricante.

- Número de 48 bits (12 dígitos hexadecimales)
- Primeros 24 bits: OUI (Organizational Unique Identifier) `http://hwaddress.com/`
- Segundos 24 bits: Serial Number



Protocolo ARP / RARP

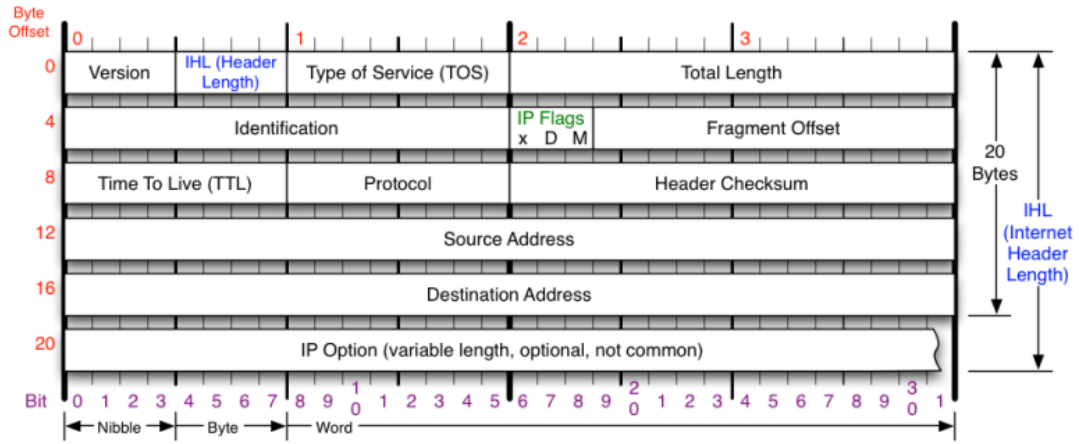
ARP (Address Resolution Protocol): Protocolo de nivel de red responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

RARP (Reverse Address Resolution Protocol): Protocolo utilizado para resolver la dirección IP de una dirección hardware dada.

Protocolo IP

El encabezado IP

IP (Internet Protocol): Protocolo no orientado a conexión para comunicar datos a través de una red de paquetes conmutada.



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

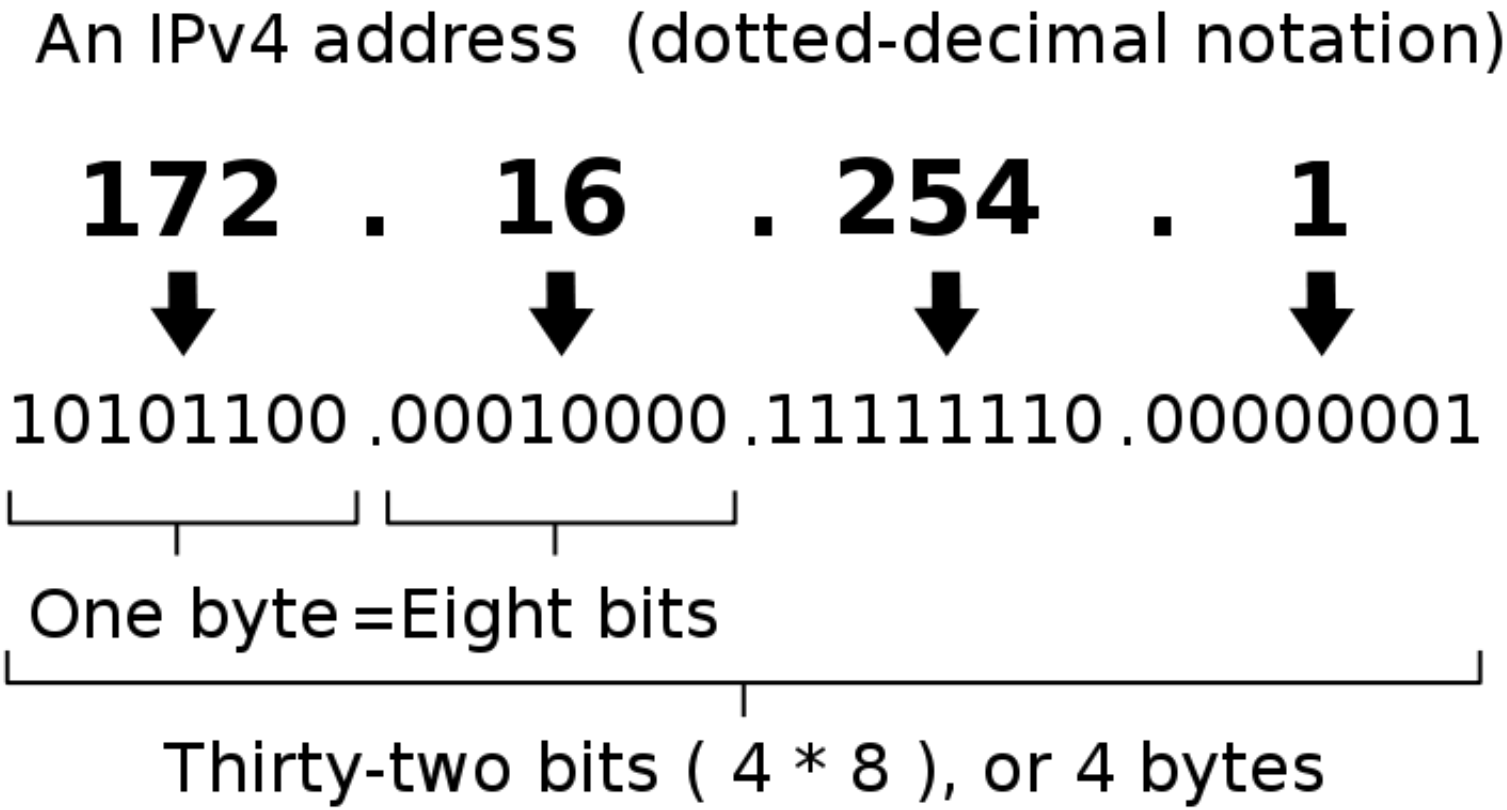
x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

Protocolo IP

Notación IP



Protocolo IP
Máscara de red

Prefijo de red

	Binary form	Dot-decimal notation
IP address	11000000.00000000.00000010.10000010	192.0.2.130
Subnet mask	11111111.11111111.11111111.00000000	255.255.255.0
Network prefix	11000000.00000000.00000010.00000000	192.0.2.0
Host identifier	00000000.00000000.00000000.10000010	0.0.0.130

Subredes

	Binary form	Dot-decimal notation
IP address	11000000.00000000.00000010.10000010	192.0.2.130
Subnet mask	11111111.11111111.11111111.**11**000000	255.255.255.192
Network prefix	11000000.00000000.00000010.10000000	192.0.2.128
Host part	00000000.00000000.00000000.00000010	0.0.0.2

Protocolo IP

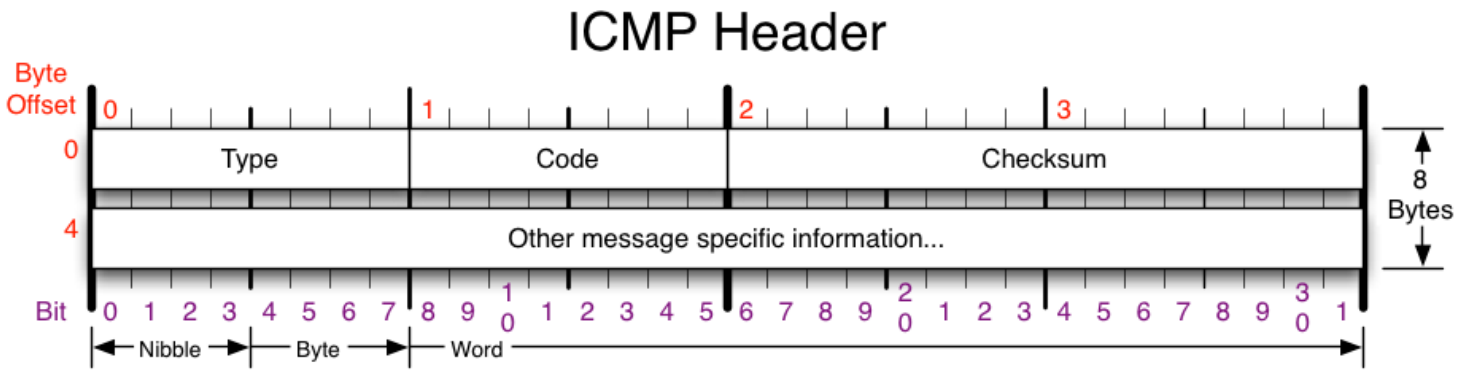
Clases de Direcciones

Clase de Dirección IP	Bits de mas peso	Intervalo 1er Octeto	Bits de dir. de red	Mascara por defecto	Parte de Red y de Host	IPs Privadas
Clase A	0	0-127	8	255.0.0.0	RRR.HHH.HHH.HHH	10.0.0.0/8
Clase B	10	128-191	16	255.255.0.0	RRR.RRR.HHH.HHH	172.16.0.0-127.31.0.0
Clase C	110	192-223	24	255.255.255.0	RRR.RRR.RRR.HHH	192.168.0.0-192.168.255.0

Protocolo ICMP

ICMP (Internet Control Message Protocol): es el sub protocolo de control y notificación de errores del Protocolo IP. Se usa para enviar mensajes de error y de control, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

Protocolo ICMP



ICMP Message Types

Type	Code/Name
0	Echo Reply
3	Destination Unreachable
	0 Net Unreachable
	1 Host Unreachable
	2 Protocol Unreachable
	3 Port Unreachable
	4 Fragmentation required, and DF set
	5 Source Route Failed
	6 Destination Network Unknown
	7 Destination Host Unknown
	8 Source Host Isolated
	9 Network Administratively Prohibited
	10 Host Administratively Prohibited
	11 Network Unreachable for TOS
3	Destination Unreachable (continued)
	12 Host Unreachable for TOS
	13 Communication Administratively Prohibited
4	Source Quench
5	Redirect
	0 Redirect Datagram for the Network
	1 Redirect Datagram for the Host
	2 Redirect Datagram for the TOS & Network
	3 Redirect Datagram for the TOS & Host
8	Echo
9	Router Advertisement
10	Router Selection
11	Time Exceded
	0 TTL Exceeded
	1 Fragment Reassembly Time Exceeded
12	Parameter Problem
	0 Pointer Problem
	1 Missing a Required Operand
	2 Bad Length
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
30	Traceroute

Checksum

Checksum of ICMP header

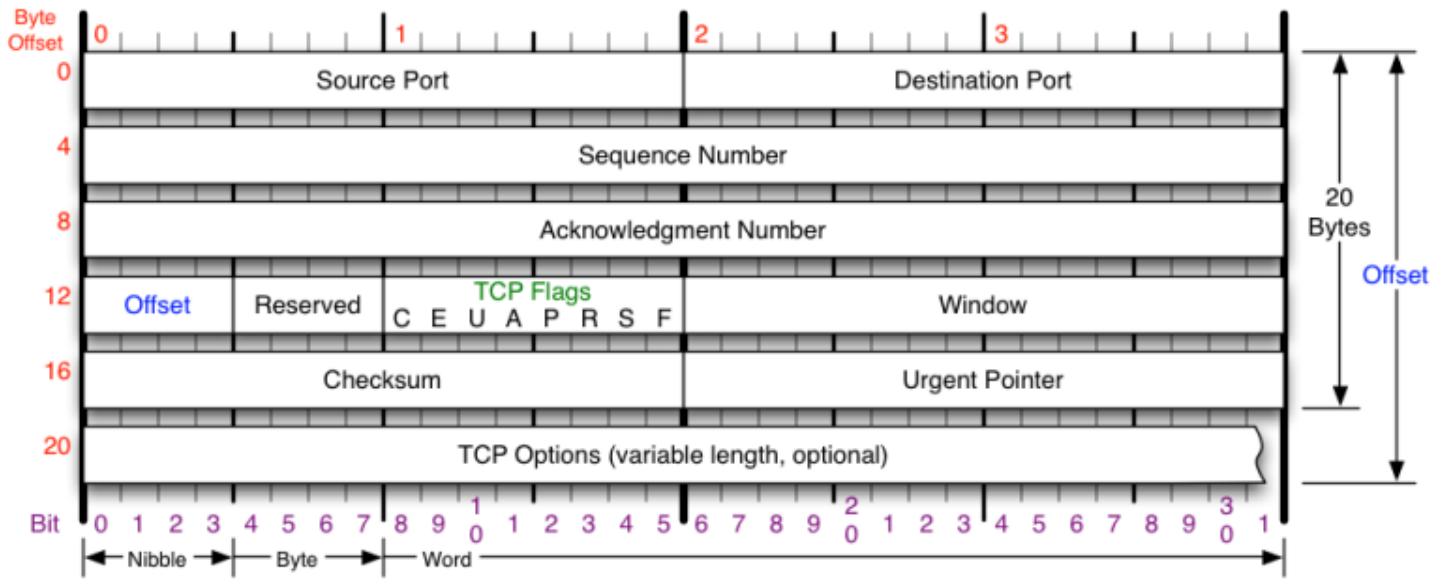
RFC 792

Please refer to RFC 792 for the Internet Control Message protocol (ICMP) specification.

Protocolo TCP

TCP (Transmission Control Protocol): provee una entrega ordenada y confiable de un flujo de bytes desde un programa en una computadora hacia otro programa en un equipo remoto (cliente-servidor).

Protocolo TCP



TCP Flags

C E U A P R S F

Congestion Window
C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

Checksum of entire TCP segment and pseudo header (parts of IP header)

Offset

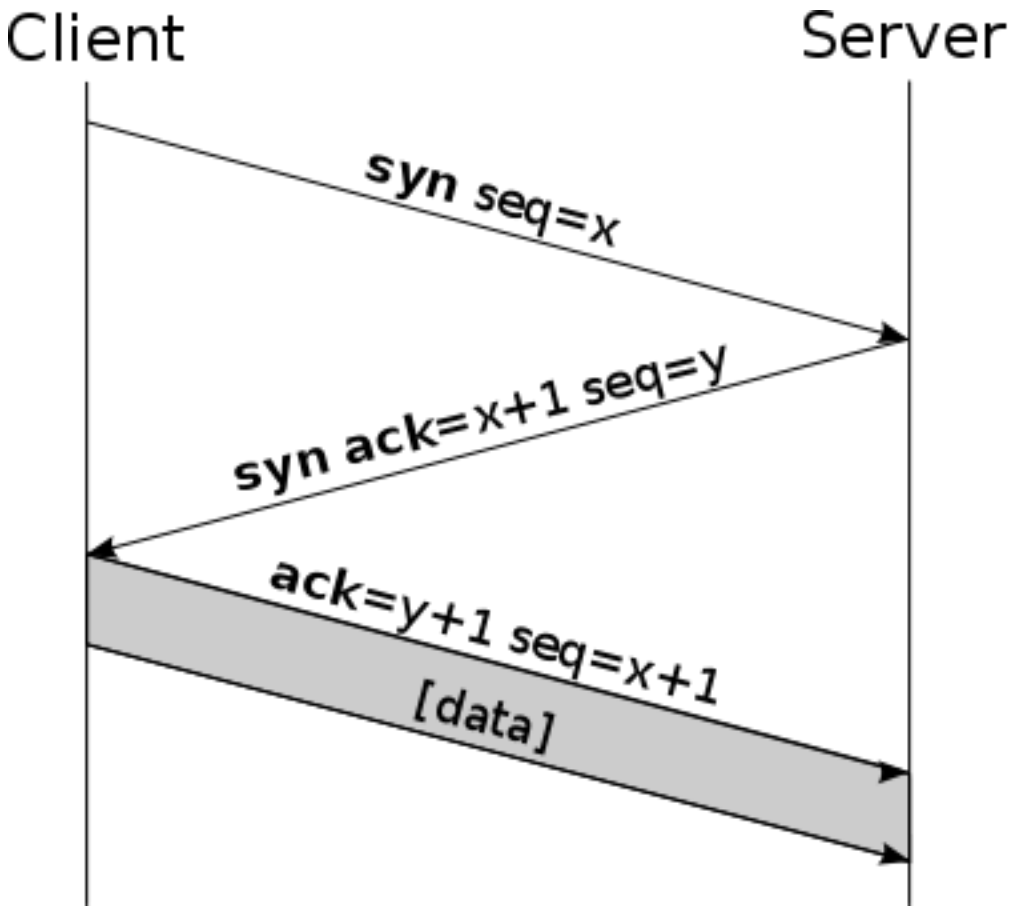
Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

RFC 793

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

Protocolo TCP

Negociación de 3 vías



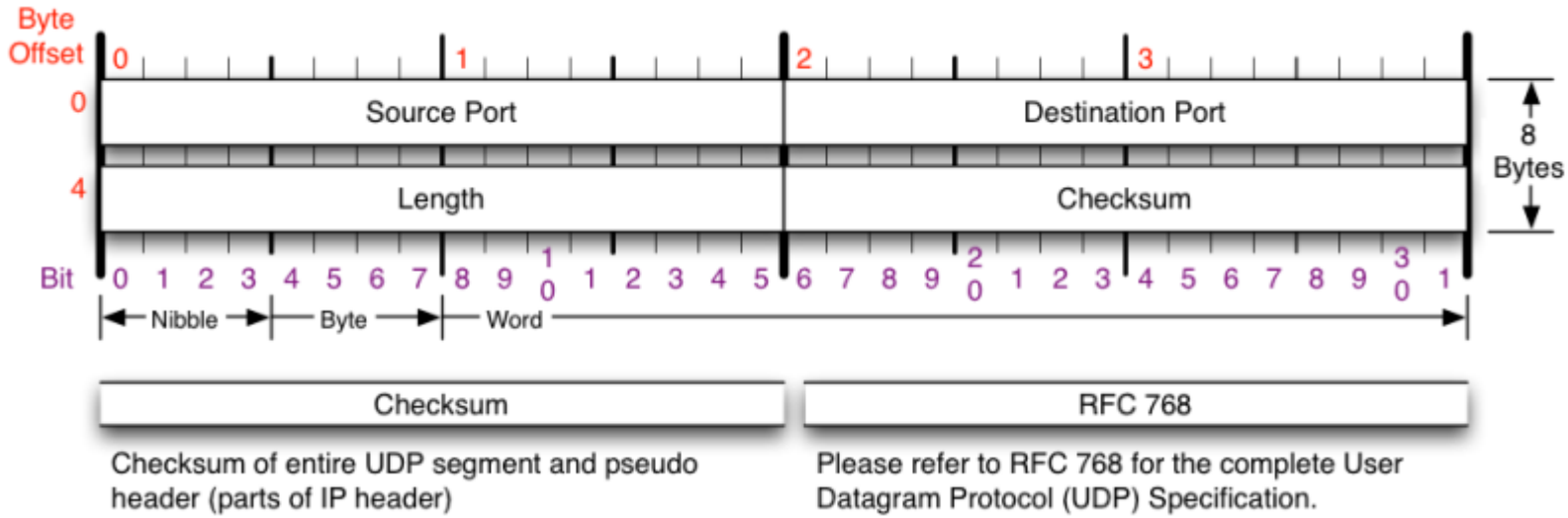
Protocolo TCP

Algunos Puertos TCP

Puerto	Descripción
20	FTP Data
21	FTP Control
22	SSH
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3
123	NTP
143	IMAP
443	HTTPS

Protocolo UDP

UDP (User Datagram Protocol): permite a las aplicaciones enviar mensajes (datagramas) a otros equipos en una red IP sin requerir el establecimiento de canales especiales de comunicación.



Nivel Aplicación

Algunas aplicaciones de Internet

Protocolo	Puerto	Descripción
FTP	20/TCP 21/TCP	**File Transfer Protocol:** se utiliza para intercambiar archivos a través de una red basada en TCP/IP.
SSH	22/TCP	**Secure SHell:** permite el intercambio de datos a través de un canal seguro entre dos dispositivos de red.
Telnet	23/TCP	Proporciona una comunicación bidireccional orientada a texto a través de una conexión de terminal virtual.
SMTP	25/TCP	**Simple Mail Transfer Protocol:** estándar para la transmisión de correo electrónico a través de redes IP.

Nivel Aplicación

Protocolo	Puerto	Descripción
DNS	53/TCP 53/UDP	**Domain Name System:** servicio distribuido que traduce nombres de dominio en direcciones numéricas IP.
DHCP	67/UDP 68/UDP	**Dynamic Host Configuration Protocol:** es utilizado por los equipos para obtener en forma dinámica una dirección IP y otros parámetros de configuración.
HTTP HTTPS	80/TCP 443/TCP	**Hyper Text Transfer Protocol:** servicio para sistemas de información distribuída y colaborativa basada en hipertexto.
POP3 POP3S	110/TCP 995/TCP	**Post Office Protocol:** permite a clientes recibir correos desde un servidor remoto.
IMAP	143/TCP 993/TCP	**Internet Message Access Protocol:** permite la publicación y acceso al servicio de correo electrónico.

Más información

- **Wikipedia**. *Modelo OSI*.
  http://en.wikipedia.org/wiki/OSI_model
- **Wikipedia**. *Modelo TCP/IP*.
  http://en.wikipedia.org/wiki/TCP/IP_model
- **Network Working Group**. *A TCP/IP Tutorial - RFC1180*.
  http://www.ietf.org/rfc/rfc1180.txt
- **NMAP**. *TCP/IP Reference*.
  https://nmap.org/book/tcpip-ref.html
- **IANA.** Internet Control Message Protocol (ICMP) Parameters.
  http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
- **Network Working Group**. *Assigned Numbers - RFC1700*.
  http://www.ietf.org/rfc/rfc1700.txt
- **Saulo Barajas**. *Curso de Protocolos TCP/IP*.
  http://www.saulo.net/pub/tcpip/index.html